ENTERPRISE CONTENT DATA RETRIEVAL

Software Assurance Supporting Information

JULY 23, 2015

BL KING CONSULTING LLC
www.blking.net

1. Enterprise Content Discovery and Retrieval

The DCGS Multi-service Execution Team Office (DMO) is a multiservice-chartered organization tasked with coordinating acquisition and implementation of the DCGS Enterprise. This coordination and implementation includes the DCGS Integration Backbone (DIB), on behalf of the DCGS programs and other DIB-user organizations. The DIB is a common set of enterprise services and standards that serves as a foundational component of the common enterprise infrastructure supporting joint and combined Intelligence Surveillance and Reconnaissance (ISR) operations. The DIB is a standards-based set of software, services, registries, configurations, documentation, and implementation processes used by participants in the DCGS Enterprise to federate distributed ISR nodes into a cohesive data-sharing environment. The DIB services execute within the Distributed Data Framework (DDF), also developed on behalf of the DMO.

The Enterprise Content Discovery and Retrieval (ECDR) Application enhances DI2E Enterprise discovery capabilities by implementing the CDR Spec & Tech Profile implementation for DDF/DIB. The app also enables greater interoperability and capabilities for data discovery as well as enhancing discovery & federation via configuration updates instead of code updates. The ECDR App easily integrates into existing production software (e.g. DCGS Integration Backbone) and helps promote adoption of the Content Discovery Retrieval (CDR) technical profiles and specifications by creating CDR capabilities as a DDF application. The app is built using open and reusable code and components and reuses existing DIB/DDF OpenSearch/CDR capabilities. Version 1.0 includes the following capabilities:

- CDR REST Search Implementation: Which is a CDR Search implementation with support for Basic Query Language
- CDR REST Brokered Search Implementation
    - Broker Federation to other CDR Services (e.g. Intelink Enterprise Catalog/Search)
    - Broker Federation with Full Legacy DIB fidelity
    - Broker Federation to Non-CDR Open Search Services
    - CDR REST Brokered Retrieve
- CDR REST Retrieve Implementation: Ability to retrieve products from the local Content Collection using CDR compliant REST Retrieve Service.

1.1. Testing Results Summary

BL King Consulting conducted security testing on the ECDR throughout the month of December. Testing included static code analysis, documentation inspection, dynamic code analysis and penetration testing. Static code analysis consisted of scanning the organic source code and third-party dependencies for vulnerabilities using HP Fortify and Coverity Security Scan with the default Java, Java Script, XML, and HTML rules enabled. Documentation inspection consisted of a comparison of the DoD Software Assurance (SwA) NIST Control Overlay and the Defense Information Systems Agency (DISA) Application Security Development Security Technical Implementation Guide

(STIG) version 3 revision 7 to the ECDRs implementation. Penetration testing was conducted using the Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP).

All issues identified by the static analysis were resolved prior to the final release. The issues that are listed as suppressed in the attached ECDR Fortify Project Summary Report are False Positives and audited as "Not an Issue". Due to the way that HP Fortify calculates the security metrics these issues are suppressed. When these issues are not suppressed HP Fortify counts these as open issues and do not reflect the true state of the project.

Penetration testing with OWASP ZAP yielded no exploitable issues. Testing identified one improvement and that improvement was to modify the input validation for passing queries to the DDF Catalog to block any queries that start with common SQL or XPATH commands, as well as any special characters. The DDF Catalog should have all the necessary precautions in place to ensure no malicious or malformed queries are accepted

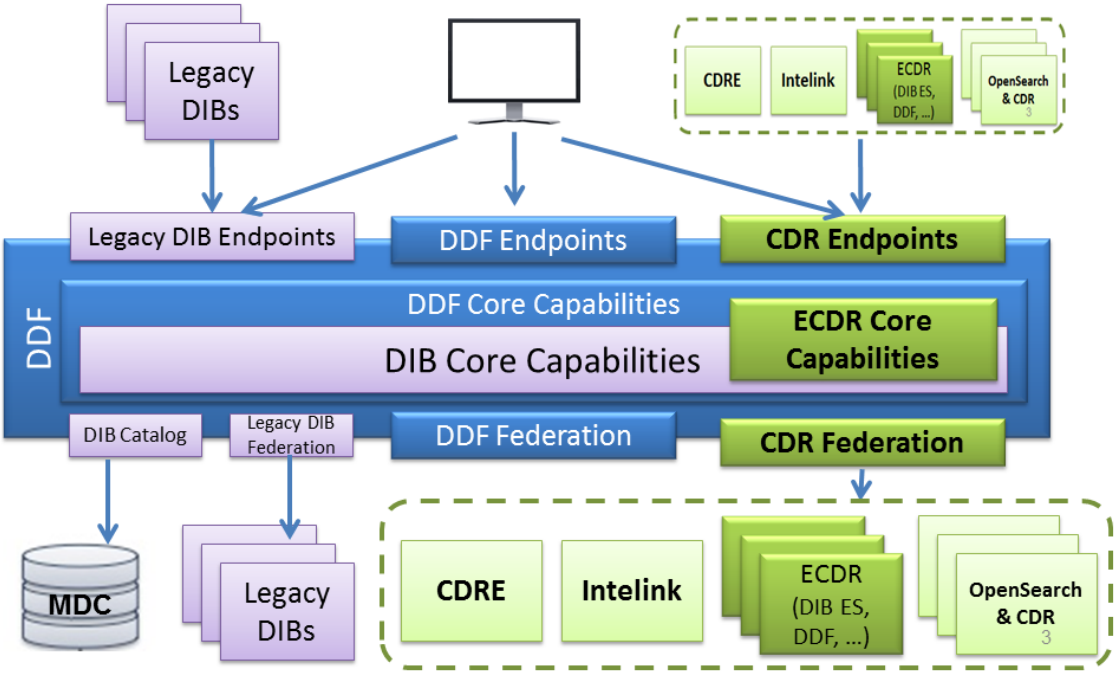
1.2. Software Assurance

The ECDR app has been evaluated using multiple DoD and Industry standards to determine the software's level of assurance. Software assurance (SwA) relates to the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software. It is unrealistic to expect software to be completely free of defects, therefore, this certification package will enumerate the known defects, and non-implemented best practices.

2. Software Overview

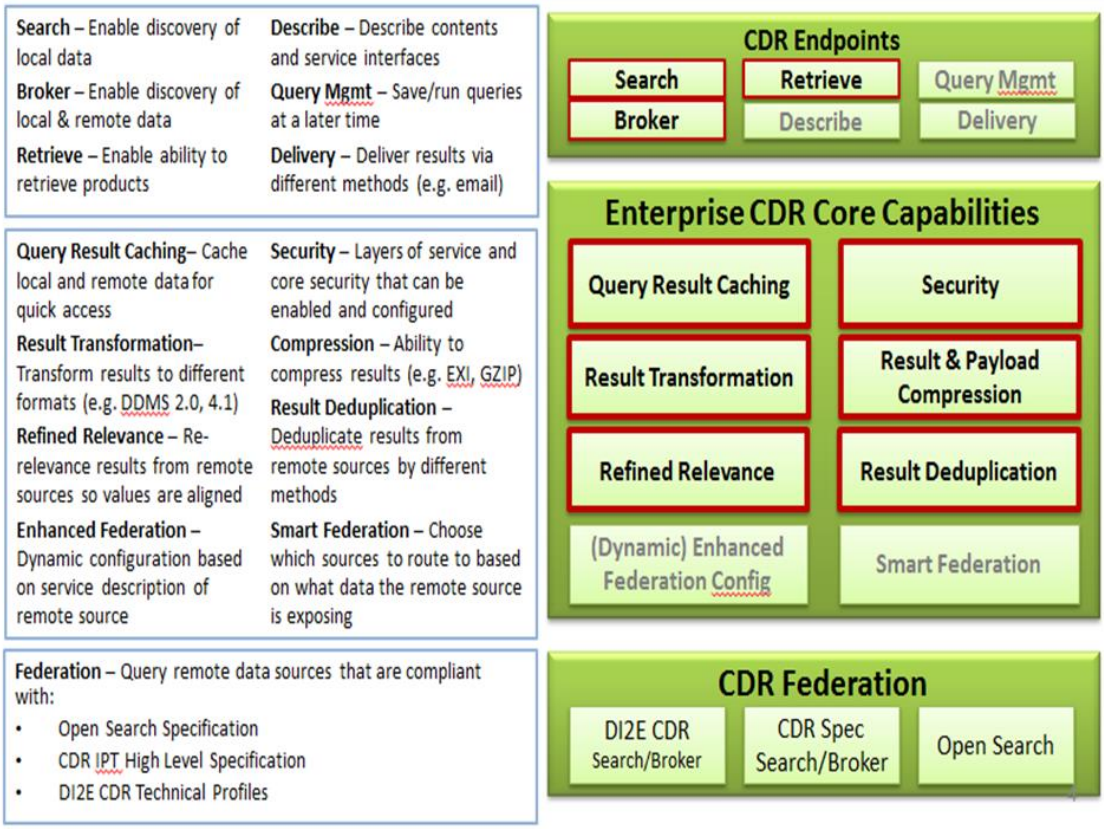
2.1. Component Overview

The Enterprise CDR Application is a DDF application that is similar to the DDF Spatial Application (which provides support for OGC Services) or the DIB Interoperability application (which provides the DIB Query Web Services and the ability to federate to other DIBs). The core difference is the Enterprise CDR Application provides support for discovering and retrieving data using the CDR Specifications (instead of the OGC or Legacy DIB Services), as can be seen in the diagram below (the green components are the Enterprise CDR Capabilities).



2.2. Component Details

Illustrated in the figure and text below are the capabilities that are included in the Enterprise CDR application. The items highlighted in red are contained in the 1.1.3 release of the Enterprise CDR application (items whose text are in gray are not currently supported, but will be in a future version).



2.3. Software Version Description

The following components are used within the ECDR Application code base.

Component Name	Version	License
ASM	4.0	BSD 3-clause
Abdera Client	1.1.3	Apache License 2.0
Abdera Core	1.1.3	Apache License 2.0
Abdera Extensions	1.13	Apache License 2.0
Axiom	1.2.14	Apache License 2.0
I18N Libraries	1.1.3	Apache License 2.0
Joda Time	2.2	Apache License 2.0
Parboiled	1.1.6	Apache License 2.0

2.4. Hosting Environment Requirements & Assumptions, Limitations, Exceptions, and Risks

2.4.1. Section Overview

This section will describe the Cyber Security policy and regulatory requirements that were either assumed to be present during the development and testing of this application or could have been deployed as an additional capability of this application, but were not developed as an included capability. These are security concerns that the intended end user or system integrator should pay particular attention to during installation and integration of this application.

Enumerating and quantifying the risk of using the Enterprise Content Discovery and Retrieval (ECDR) App in a potential environment is impossible from a development standpoint due to the near infinite permutations of differing software that is used to host the software. For example, one end user may use RedHat 4.5, with one security configuration, running DDF 2.0 with one security configuration whereas another customer may be running Windows Server 2003 and DDF 2.2 with customization. The objective of the Test Report is to identify what security features ECDR implements and how well it does, whereas this section is focused on what ECDR does not do that is of a security concern. There is a subset of this guidance that is impractical for the ECDR software to implement and thus that risk cannot be assessed from a pure ECDR perspective.

The user that is implementing the ECDR should review this section in context with their chosen software and system baseline to identify the total system risk. Comparing the items that ECDR does not implement with the users chosen implementation will identify security gaps. Those gaps should be assessed for system level risk impact to enable an informed risk decision.

	Capability Provided	**Interoperable with Capability Provider**	**No Capability**
Identification and Authentication			X
Authorization			X
Redundancy			X
Intrusion Detection			x
Firewall			x
Non-Repudiation			x
Automatic Security Labels (In-Transit)			x
Automatic Security Labels (At Rest)			x
Manual Security Labels (In-Transit)			x

	Capability Provided	Interoperable with Capability Provider	No Capability
Manual Security Labels (At Rest)			x
Public Key Encryption			x
Public Key Infrastructure			x
Encryption Key Stores			x
File Access Control Lists			x

Assumptions

During development, testing, and certification certain assumptions were made; care was taken to document these assumptions. However this list is not all inclusive:

- Database Applications are secured by the end user or system integrator
- The hosting environment has the appropriate security authorization to operate
- Encryption for data at rest is accomplished by the end user or system integrator

Requirements Trace-ability

The intended operating environment for the Virtual MetaData Catalog (ECDR) is a DoD or equivalent, assessed, and authorized enclave. This software was functionally tested using DoD hardened (e.g. DISA STIG) operating systems for both client and servers. Any known required deviations from DISA STIG's are noted in later sub-sections.

Evaluation criteria for the ECDR are derived from NIST SP 800-53 Rev 4. The DoD Risk Management Framework (RMF) Technical Advisory Group (TAG) approved Web Application Overlay was used to evaluate the ECDR. These criteria along with their implementation status are documented in both the Test Results Summary as well as the Security Requirements Trace.

2.4.2. Exceptions

The following exceptions to common security guidance is required for Enterprise CDR to operate properly:

- No Known exceptions

2.4.3. Vulnerabilities

No vulnerabilities were identified with the ECDR App.

3. Security Test Report

3.1. Executive Summary

The DCGS Multi-service Execution Team Office (DMO) is a multiservice-chartered organization tasked with coordinating acquisition and implementation of the DCGS Enterprise, including the DCGS Integration Backbone (DIB), on behalf of the DCGS programs and other DIB-user organizations. The DIB is a common set of enterprise services and standards that serves as a foundational component of the common enterprise infrastructure supporting joint and combined Intelligence Surveillance and Reconnaissance (ISR) operations. The DIB is a standards-based set of software, services, registries, configurations, documentation, and implementation processes used by participants in the DCGS Enterprise to federate distributed ISR nodes into a cohesive data-sharing environment. The DIB services execute within the Distributed Data Framework (DDF), also developed on behalf of the DMO. The Enterprise Content Discovery and Retrieval (ECDR) Application enhances DI2E Enterprise discovery capabilities by implementing the CDR Spec & Tech Profile implementation for DDF/DIB. The app also enables greater interoperability and capabilities for data discovery as well as enhancing discovery & federation via configuration updates instead of code updates. The ECDR App easily integrates into existing production software (e.g. DCGS Integration Backbone) and helps promote adoption of the Content Discovery Retrieval (CDR) technical profiles and specifications by creating CDR capabilities as a DDF application. The app is built using open and reusable code and components and reuses existing DIB/DDF OpenSearch/CDR capabilities. Version 1.0 includes the following capabilities:

- CDR REST Search Implementation: Which is a CDR Search implementation with support for Basic Query Language
- CDR REST Brokered Search Implementation
    - Broker Federation to other CDR Services (e.g. Intelink Enterprise Catalog/Search)
    - Broker Federation with Full Legacy DIB fidelity
    - Broker Federation to Non CDR Open Search Services
    - CDR REST Brokered Retrieve
- CDR REST Retrieve Implementation: Ability to retrieve products from the local Content Collection using CDR compliant REST Retrieve Service.

Figure 1 Figure 1 Software Architecture

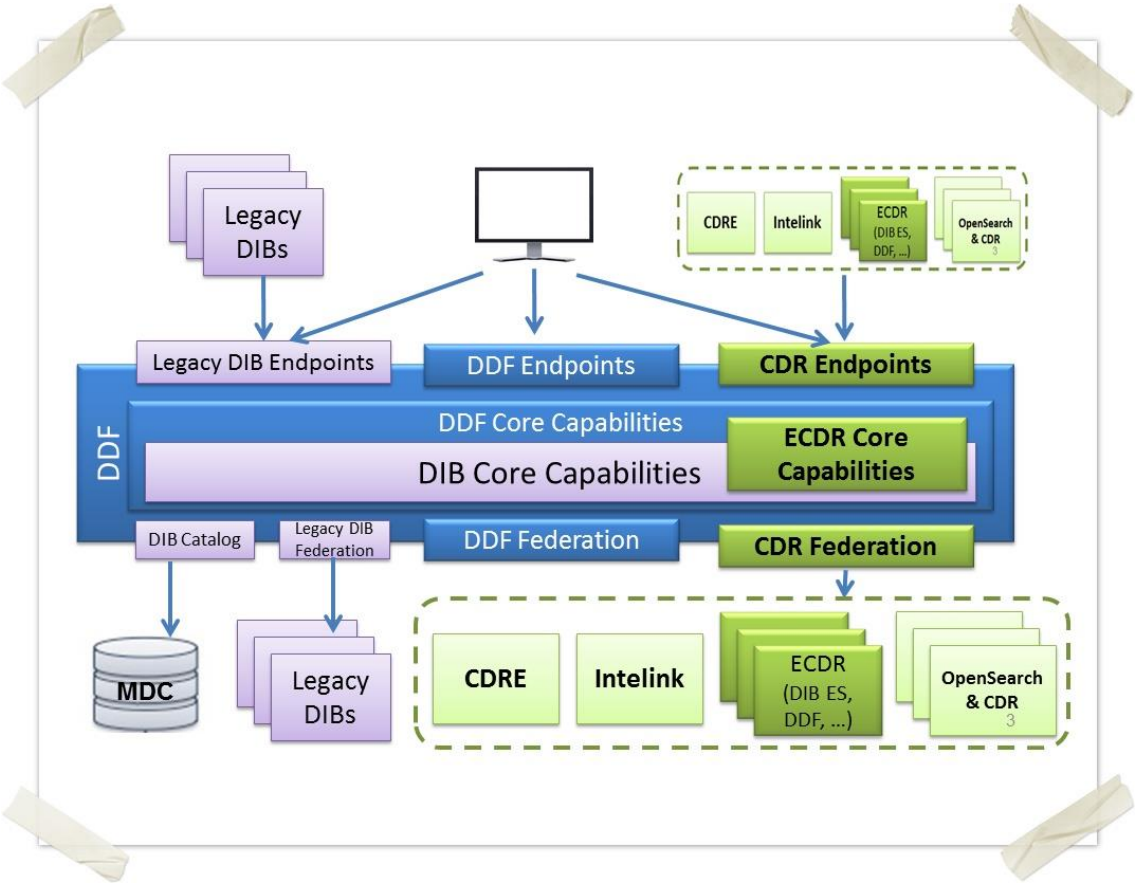


Figure 1 Software Architecture

BL King Consulting LLC conducted security testing on the ECDR throughout the month of December. Testing included static code analysis, documentation inspection, dynamic code analysis, and penetration testing. Static code analysis consisted of scanning the organic source code and third-party dependencies for vulnerabilities using HP Fortify and Coverity Security Scan with the default Java, Java Script, XML, and HTML rules enabled. Documentation inspection consisted of a comparison of the DoD Software Assurance (SwA) NIST Control Overlay and the Defense Information Systems Agency (DISA) Application Security Development Security Technical Implementation Guide (STIG) version 3 revision 7 to the ECDRs implementation. Penetration testing was conducted using the Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP).

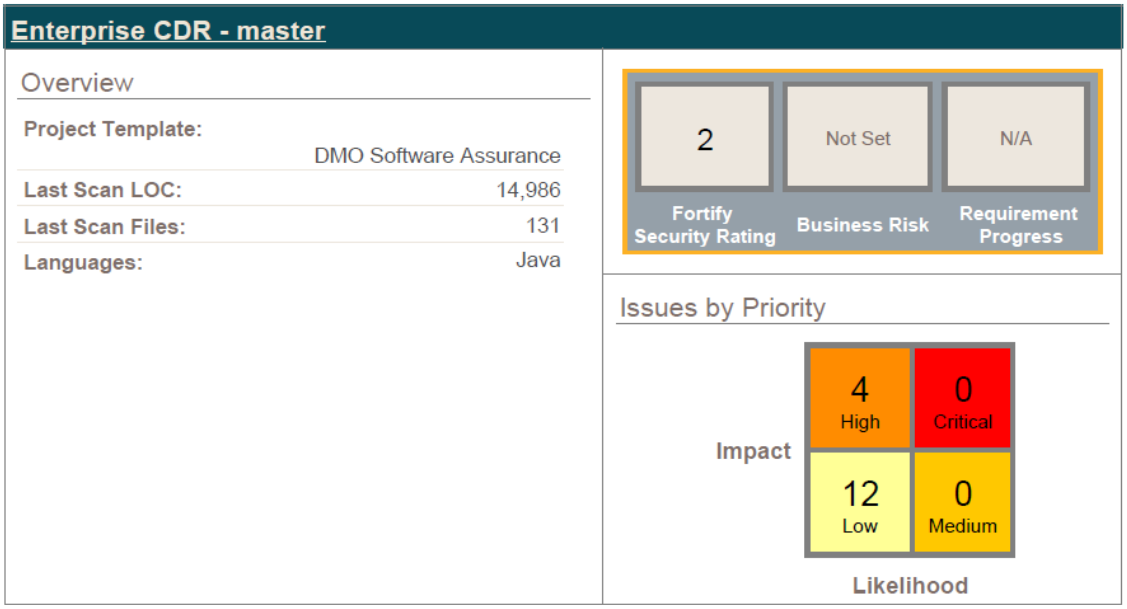
All issues identified by the static analysis were resolved prior to the final release. The issues that are listed as suppressed in the attached ECDR Fortify Project Summary Report are issues that were identified as False Positives and audited as "Not an Issue". Due to the way that HP Fortify calculates the security metrics these issues were suppressed. When these issues were not suppressed HP Fortify counted these as open issues and did not reflect the true state of the project.

Penetration testing with OWASP ZAP yielded no exploitable issues. One improvement was identified, and that improvement was to modify the input validation for passing queries to the DDF Catalog to block any queries that start with common SQL or XPATH commands, as well as any special characters. The DDF Catalog should have

all the necessary precautions in place to ensure no malicious or malformed queries are accepted.

Static Analysis of the ECDR code resulted in an overall HP Fortify Rating of 2 (this indicates issues with the rating of "high") see Figure 2 Static Analysis Summary. 16 issues were found.

Figure 2 Static Analysis Summary



3.2. Scope

ECDR 1.1.3 source code, binaries, and documentation were evaluated during this assessment. Supporting software, to include the framework, operating system, and network infrastructure were not evaluated during this assessment. The green blocks in Figure 1 ECDR Component Overview are the ECDR application that is the subject of this assessment.

3.3. Objectives

The primary objective of this assessment is to identify what best practices, capabilities, and risks exist within the ECDR software. As no compliance mandate exists for software, there is no evaluation as to compliance levels. This assessment will give the reviewer (e.g. IAM/ISSM, CA, DAA, System Integrator, Program Manager, End User) the ability to understand the risks that this software poses to their environment.

3.3.1. Objective 1: Security Relevant Code Flaws

A key component to Software Assurance is the underlying source code, and the quality instilled by the developers. This assessment will identify and enumerate code flaws from all code sources, to include third-party code that is present during runtime.

3.3.2. Objective 2: NIST Control Evaluation

The National Institute of Standards and Technology (NIST) has published a series of controls that, when implemented, will enhance an information technology products cyber security risk posture. This assessment will evaluate the implementation of the SwA Controls overlay by the ECDR.

3.3.3. Objective 3: Application Security and Development STIG Evaluation

The Defense Information Systems Agency has developed technical guidance for application developers. This assessment will evaluate ECDRs implementation of the guidance provided by the DISA ASD STIG.

3.3.4. Objective 4: Dynamic Program Analysis / Penetration Testing

This objective aims to find common issues with the app in a running environment. Some issues will not be found in static analysis, threat modeling, or peer code reviews. This objective tests the application against common attack patterns. Results from this testing are typically exploitable and present with the highest priority.

3.4. Methodology

Evaluation of the ECDR will include gathering information from multiple sources.

- Objective 1
    - HP Fortify Static Code Analyzer will be used with the default rules from HP that were current as of the date of testing January 2014.
    - Findbugs will also be used to assess source code with the HP Fortify scan engine.
    - Issues that are identified will be audited by the development team and the development security architect to remove false positives
    - The HP Provided DISA STIG report will be used to allocate audited issues to STIG guidance, this report contains a many-to-many relationship where many issues can map to many STIG guidance and thus will not be used as the single source report.
    - To supplement the HP Fortify static analysis, Coverity will be used to scan the app for issues that HP Fortify did not catch. This tool does not have a reporting capability.
- Objective 2/3
    - Documentation Inspection

        - The documentation for the ECDR software is available at https://confluence.di2e.net/display/ECDR/ECDR+Application+v1.0+User+Guide. This documentation will be inspected to gather information for the stated objectives.
        - Functional Testing
            - Where applicable, functional testing of capabilities will be tested by the Development security architect to ensure capabilities perform as expected.

- Objective 4
    - The ECDR App will be deployed on a CENTOS 7 server running JAVA 7 and DIB Enterprise Suite 4.1 and tested using the OWASP ZED Attack Proxy. Requests will be proxied from a workstation Firefox browser through a separate Penetration testing virtual machine running Kali Linux Distribution (latest).
    - The following queries will be fuzz tested for each parameter.
        - http://192.168.65.128:8181/services/cdr/search/rest?q=Predator
        - http://192.168.65.128:8181/services/cdr/search/rest?q=predator&caseSensitive=1
        - http://192.168.65.128:8181/services/cdr/search/rest?q=predator&caseSensitive=1&fuzzy=1
        - http://192.168.65.128:8181/services/cdr/search/rest?q=predator&caseSensitive=1&fuzzy=1&dtStart=2013-01-01T00:00:00-00:00&dtEnd=2015-01-01T00:00:00-00:00
        - http://192.168.65.128:8181/services/cdr/search/rest?q=predator&caseSensitive=1&fuzzy=1&dtStart=2013-01-01T00:00:00-00:00&dtEnd=2015-01-01T00:00:00-00:00&dtType=updated
        - http://192.168.65.128:8181/services/cdr/search/rest?q=Predator&polygon=45.2,-110.4,46.4,-109.4,43.8,-109.8,45.2,-110.4
        - http://192.168.65.128:8181/services/cdr/search/rest?q=Predator&geometry=POLYGON((30 10, 40 40, 20 40, 10 20, 30 10))
    - It is assumed, from a security perspective, that the brokered search logic will perform in the same manner, and thus fuzz testing is not repeated for the brokered search.
    - Issues identified that are outside of the /services/cdr/ sub-tree are considered out of scope for this objective.
    - The /services/cdr/ sub tree will be enumerated using a forced browsing method. This method uses a list of common directory structures and tries each from the list.
    - The /services/cdr sub tree will be further enumerated using a web spider. This method reads URLs from each page and follows each link to enumerate all linked pages.

- The /services/cdr sub tree will be attacked using common attack patterns from the Active Scan feature within OWASP ZAP.

All analysis of results is considered agnostic of the operating environment to ensure an un-biased assessment with as few unintended assumptions as possible. This method will ensure that the results of this assessment are applicable to as many operating environments as possible.

3.5. Results Summary

- Objective 1: Static Code Analysis
  - During mid-development, initial testing man issues were identified.
  - Over the course of the development, many of these issues were determined to be false positives.
  - By the end of the development, all issues had been resolved.
- Objective 2/3:
  - A thorough evaluation of the ECDR application was conducted using the DoD Software Assurance Web App overlay and the DISA AS&D STIG.
  - For the controls and STIG items that the ECDR application or ECDR Developer were responsible for only a few failed.
    - AU-9
      - The application sends the contents of user entered fields to the DDF Log.
      - This is considered a moderate risk as the unvalidated text could be read by the a log viewer as code.
      - The simplest mitigation is to restrict access to ECDR to authorized and authenticated users.
    - CM-1 and CM-9
      - No developer level CM plan exists
      - This is considered a low risk due to the size of the team and the use of a software configuration control product (Git Hub).
    - SA-15 and SA-15(1)
      - No Software Development Plan Exists
      - Quality metrics was not defined at the beginning of the development
      - This is considered a low risk as quality issues were resolved as evidenced by HP Fortify and Coverity (both of which look at code quality).

    - SA-15(6)
        - The development team has not implemented an explicit process for continuous improvement
        - This is considered a low risk as the development team consists of 2 developers and 1 security architect
    - SA-4(3)/V=21519
        - ECDR uses Open Source Software which may go unsupported if the OSS community stops supporting the products
        - This is considered a low risk as the developer has access to the source code if support were to fail and were needed by customers of ECDR

- Objective 4:
    - Many server issues were identified; however, they were out of scope as they pertained to the DDF, not the ECDR.
    - FUZZ testing revealed the only item of concern. However this is considered an improvement and not a risk or bug.
    - When the ECDR passes queries to the DDF Catalog, almost all text is passed to the DDF Catalog. If the DDF Catalog does not adequately perform input validation then this text, which could be malicious, could be passed to the data store and executed as code.
    - The ECDR app could implement input validation on the query text to ensure that malicious code is not passed to the DDF Catalog.

4. Hardening Checklist

This checklist will guide the Information System Security Officer or System Administrator in securing the DDF to protect the Enterprise Content Discovery Retrieval (ECDR) application.

1. Ensure that the <DDF Install> directory and sub-directories limit access to only ddf-user and system administrators.
2. Enable Web Service Security and ensure clients are authenticated prior to accessing the ECDR Endpoints.
3. Ensure the hosting server and network are appropriately secured and authorized.
4. Enable Transport Layer Security on the DDF for the ECDR endpoints.

5. Enable Identification and Authentication for embedded data stores.

These security mitigations are based upon the ECDR Threat Model and are required to mitigate specific threats to the ECDR application. If the end user chooses not to implement one of these mitigations, then the end user will need to consider this as a risk and update their risk profile.

5. Users, Access, and Auditing

There is no requirement by the ECDR app for any new/unique user. Access to the ECDR app is controlled by the DDF and the implemented security policy. Auditing of security relevant events should be processed by the DDF.

6. Ports, Protocols, and Services

The following describes the network communications that are used by the ECDR App. As noted below these are user/integrator configurable and can be modified as appropriate.

The following is a list of protocols required for the ECDR App.

Service or Application	Port and Protocol	User and Justification	Service internal to the LAN	Service outside the boundary of the LAN	DSAWG Rating
**http	*/tcp	Client connection to ECDR REST Endpoint	**	**	Yellow
**https	443/tcp	Client connection to ECDR REST Endpoint	**	**	Green

*Port is select-able by the end user or system integrator of the specific implementation in the DDF configuration.

**Configuration option dependent upon security requirements and mission needs

7. ECDR Mobile Code

No mobile code is included in the ECDR application. All code is executed on the server.

8. Signature

The contents of this documentation are a true and factual representation of my analysis and assessment.

Bobby King Jr.

Bobby King

Digitally signed by Bobby King
Date: 2015.07.23 21:35:00 -04'00'

9. Appendices

9.1. Threat Model

The following introduction was retrieved from https://www.owasp.org/index.php/Application_Threat_Modeling on 18 November 2013.

"Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application. Threat modeling is not an approach to reviewing code, but it does complement the security code review process. The inclusion of threat modeling in the SDLC can help to ensure that applications are being developed with security built-in from the very beginning. This, combined with the documentation produced as part of the threat modeling process, can give the reviewer a greater understanding of the system. This allows the reviewer to see where the entry points to the application are and the associated threats with each entry point. The concept of threat modeling is not new, but there has been a clear mindset change in recent years. Modern threat modeling looks at a system from a potential attacker's perspective, as opposed to a defender's viewpoint. Microsoft have been strong advocates of the process over the past number of years. They have made threat modeling a core component of their SDLC, which they claim to be one of the reasons for the increased security of their products in recent years.

When source code analysis is performed outside the SDLC, such as on existing applications, the results of the threat modeling help in reducing the complexity of the source code analysis by promoting an in-depth first approach vs. breadth first approach. Instead of reviewing all source code with equal focus, you can prioritize the security code review of components whose threat modeling has ranked with high risk threats.

The threat modeling process can be decomposed into 3 high level steps:

***Step 1:** Decompose the Application. The first step in the threat modeling process is concerned with gaining an understanding of the application and how it interacts with external entities. This involves creating use-cases to understand how the application is used, identifying entry points to see where a potential attacker could interact with the application, identifying assets i.e. items/areas that the attacker would be interested in, and identifying trust levels which represent the access rights that the application will grant to external entities. This information is documented in the Threat Model document and it is also used to produce data flow diagrams (DFDs) for the application. The DFDs show the different paths through the system, highlighting the privilege boundaries.*

***Step 2:** Determine and rank threats. Critical to the identification of threats is using a threat categorization methodology. A threat categorization such as STRIDE can be used, or the Application Security Frame (ASF) that defines threat categories such as Auditing & Logging, Authentication, Authorization, Configuration Management, Data Protection in Storage and Transit, Data Validation, Exception Management. The goal of the threat categorization is to help identify threats both from the attacker (STRIDE) and the defensive perspective (ASF). DFDs produced in step 1 help to identify the potential threat targets from the attacker's perspective, such as data sources, processes, data flows, and interactions with users. These threats can be identified further as the roots for threat trees; there is one tree for each threat goal. From the defensive perspective, ASF categorization helps to identify the threats as weaknesses of security controls for such threats. Common threat-lists with examples can help in the identification of such threats. Use and abuse cases can illustrate how existing protective*

measures could be bypassed, or where a lack of such protection exists. The determination of the security risk for each threat can be determined using a value-based risk model such as DREAD or a less subjective qualitative risk model based upon general risk factors (e.g. likelihood and impact).

***Step 3:** Determine countermeasures and mitigation. A lack of protection against a threat might indicate a vulnerability whose risk exposure could be mitigated with the implementation of a countermeasure. Such countermeasures can be identified using threat-countermeasure mapping lists. Once a risk ranking is assigned to the threats, it is possible to sort threats from the highest to the lowest risk, and prioritize the mitigation effort, such as by responding to such threats by applying the identified countermeasures. The risk mitigation strategy might involve evaluating these threats from the business impact that they pose and reducing the risk. Other options might include taking the risk, assuming the business impact is acceptable because of compensating controls, informing the user of the threat, removing the risk posed by the threat completely, or the least preferable option, that is, to do nothing.*

Each of the above steps are documented as they are carried out. The resulting document is the threat model for the application."

The Threat Model for the ECDR app was developed using the STRIDE methodology with risk values assigned using the DREAD model. Security professionals using the output from this threat model should take note that the risk model is subjective and is agnostic of the hosting environment. To consider the risk to the hosting information system or hosting environment a system-level risk assessment must be completed, and should include information gathered from the ECDR, threat model.

9.1.1. Threat Modeling Report

Created on 12/20/2014 7:21:29 PM

Threat Model Name: ECDR Version 1.1.3 Threat Model

Owner: Bobby King

Reviewer: Jeff Vettraino, Matthew Ramey

Contributors: Bobby King

Description: The ECDR application receives DDF Catalog queries in a REST format and provides that query to the DDF Catalog, then receives the response from the DDF Catalog and provides that to the client via REST.

Assumptions: It is assumed that the ECDR App will be installed on a properly secured system and within a properly secured network that will properly secure the file system and prevent unauthenticated/unauthorized access to the file system. It is also assumed that the hosting environment will be able to prevent most Denial of Service attacks.

External Dependencies:

9.1.2. Notes:

Id	Note	Date	Added By
1	Need to determine how logging works within the DDF. Notice that what is displayed on /system/console/events is not stored in a .log file in the file system. It's unknown where it is stored.	12/20/2014 5:47:53 PM	Bobby

9.1.3. Threat Model Summary:

Not Started	0
Not Applicable	10
Needs Investigation	12
Mitigation Implemented	37
Total	59
Total Migrated	0

Diagram: Diagram 1

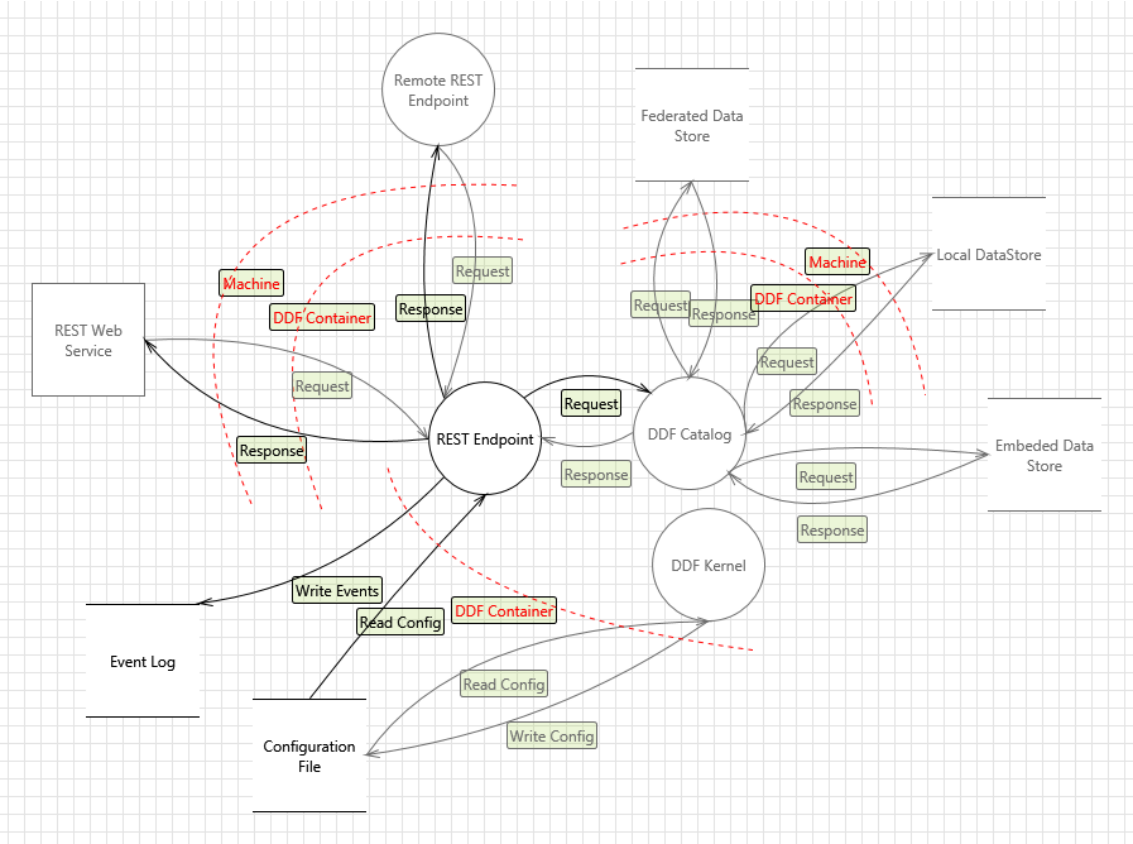


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	10
Needs Investigation	12
Mitigation Implemented	37
Total	59

Total Migrated	0

Threat(s) Not Associated With an Interaction:

1. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	REST Endpoint may be able to impersonate the context of DDF Catalog in order to gain additional privilege.
Justification:	ECDR and DDF Catalog operate at the same permission level.

2. REST Endpoint Process Memory Tampered [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	If REST Endpoint is given access to memory, such as shared memory or pointers or is given the ability to control what DDF Catalog executes (for example, passing back a function pointer.), then REST Endpoint can tamper with DDF Catalog. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification:	Memory management is handled by the Java Virtual Machine.

3. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	DDF Catalog may be able to impersonate the context of REST Endpoint in order to gain additional privilege.
Justification:	DDF Catalog and ECDR REST Endpoint run with the same privileges.

4. Spoofing of Destination Data Store File System [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

Description:	File System may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.
Justification:	Ensure File System Permissions restrict access to only trusted administrators. (ECDR Mitigation #1 – Hardening Checklist)

5. Potential Excessive Resource Consumption for REST Endpoint or File System [State: Needs Investigation] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	Does REST Endpoint or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification:	Added to ECDR Backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-76

6. Spoofing the REST Endpoint Process [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	REST Endpoint may be spoofed by an attacker, and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process.
Justification:	The ECDR Rest Endpoint resides on the same machine as the File System

7. The File System Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Data flowing across Binary may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store.
Justification:	Ensure File System Permissions restrict access to only trusted administrators (ECDR Mitigation #1 – Hardening Checklist)

8. Data Store Denies File System Potentially Writing Data [State: Not Applicable] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time and summary of the received data.
Justification:	This threat appears to be an MS TMT anomaly.

9. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.
Description:	Data flowing across Binary may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification:	Ensure File System Permissions restrict access to only trusted administrators (ECDR Mitigation #1 – Hardening Checklist)

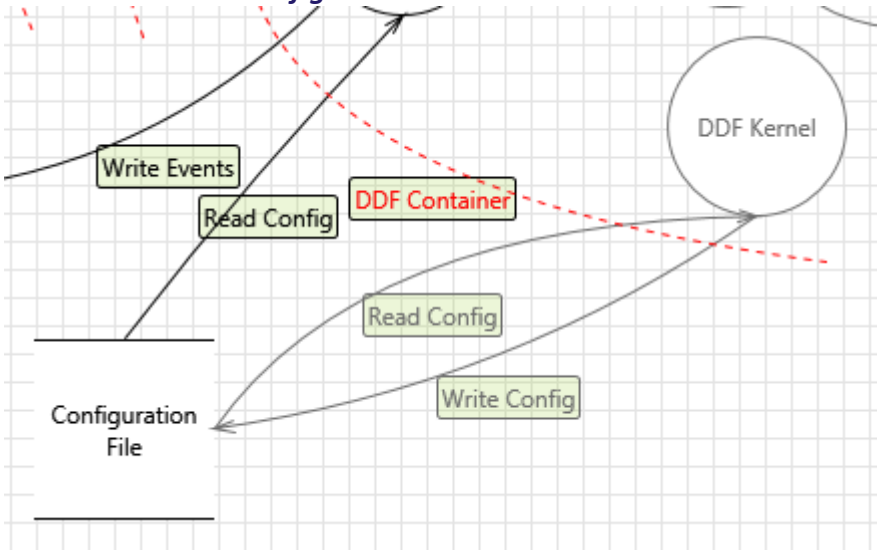
10. Data Flow Binary Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	Ensure File System Permissions restrict access to only trusted administrators (ECDR Mitigation #1 – Hardening Checklist)

11. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent prevents access to a data store on the other side of the trust boundary.
Justification:	Ensure File System Permissions restrict access to only trusted administrators (ECDR Mitigation #1 – Hardening Checklist)

Interaction: Read Config



12. DDF Kernel May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	Configuration File may be able to remotely execute code for DDF Kernel.
Justification:	DDF Kernel Threats are out of scope for this threat model.

13. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent prevents access to a data store on the other side of the trust boundary.
Justification:	Configurations for ECDR are default search parameters. If that configuration file were to be inaccessible, the app would rely on the original defaults to perform queries.

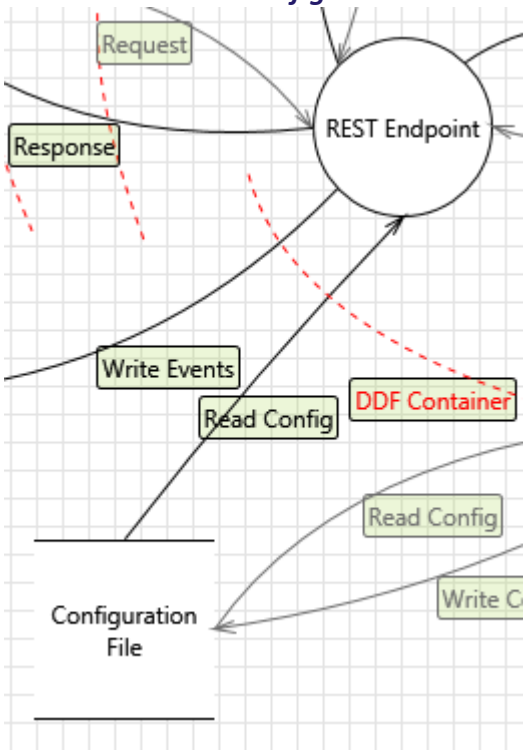
14. Data Flow Binary Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	DDF Kernel, ECDR App, and the configuration file reside on the same machine.

15. Potential Process Crash or Stop for DDF Kernel [State: Not Applicable] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	DDF Kernel crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification:	DDF Kernel threats are outside of the scope of this threat model.

Interaction: Read Config



16. Elevation by Changing the Execution Flow in REST Endpoint [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	An attacker may pass data into REST Endpoint in order to change the flow of program execution within REST Endpoint to the attacker's choosing.
Justification:	All input is processed by an input validator. Furthermore, each input is fuzz tested prior to release.

17. REST Endpoint May be Subject to Elevation of Privilege Using Remote Code Execution [State: Needs Investigation] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.

Description:	Configuration File may be able to remotely execute code for REST Endpoint.
Justification:	Added to ECDR Backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-77

18. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent prevents access to a data store on the other side of the trust boundary.
Justification:	Both Configuration File and REST Endpoint reside on the same machine.

19. Data Flow Binary Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	Both REST Endpoint and Configuration file reside on the same machine.

20. Potential Process Crash or Stop for REST Endpoint [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	REST Endpoint crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification:	During development, static analysis for security and quality is performed and reviewed to ensure that reliability concerns are addressed prior to a release.

21. Potential Data Repudiation by REST Endpoint [State: Not Applicable] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.

Description:	REST Endpoint claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time and summary of the received data.
Justification:	Repudiation of reading the configuration file is not a concern.

22. Spoofing the REST Endpoint Process [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	REST Endpoint may be spoofed by an attacker, and this may lead to information disclosure by Configuration File. Consider using a standard authentication mechanism to identify the destination process.
Justification:	The configuration file contains no sensitive data.

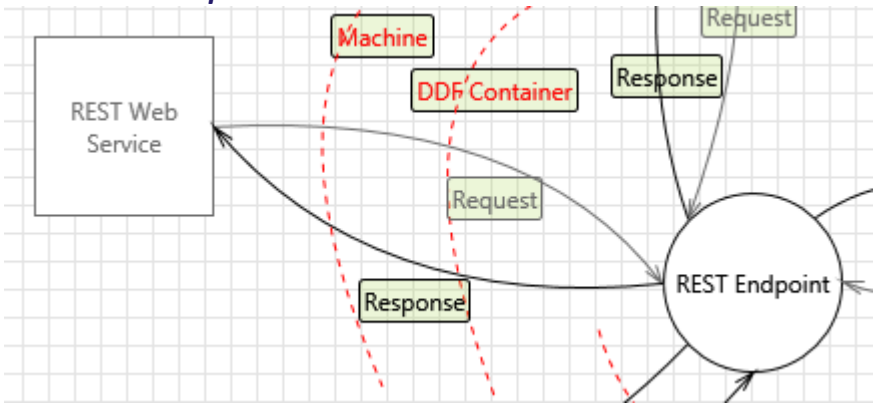
23. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.
Description:	Improper data protection of Configuration File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification:	The configuration file contains no sensitive data.

24. Spoofing of Source Data Store Configuration File [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	Configuration File may be spoofed by an attacker, and this may lead to incorrect data delivered to REST Endpoint. Consider using a standard authentication mechanism to identify the source data store.
Justification:	The ECDR and configuration file reside on the same machine.

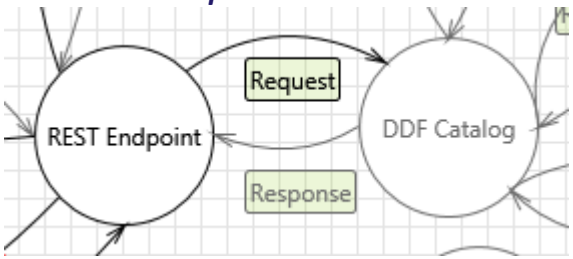
Interaction: Request



25. Spoofing the REST Endpoint Process [State: Needs Investigation] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	REST Endpoint may be spoofed by an attacker, and this may lead to information disclosure by REST Web Service. Consider using a standard authentication mechanism to identify the destination process.
Justification:	Enable Web Service Security and ensure clients are authenticated prior to accessing the ECDR Endpoints.(ECDR Mitigation #2 – Hardening Checklist)

Interaction: Request



26. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	DDF Catalog may be able to impersonate the context of REST Endpoint in order to gain additional privilege.
Justification:	Both REST Endpoint and DDF Catalog reside within the same application container and run with the same privileges.

27. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.
Justification:	Both REST Endpoint and DDF Catalog reside within the same application container.

28. Replay Attacks [State: Mitigation Implemented] [Priority: High]

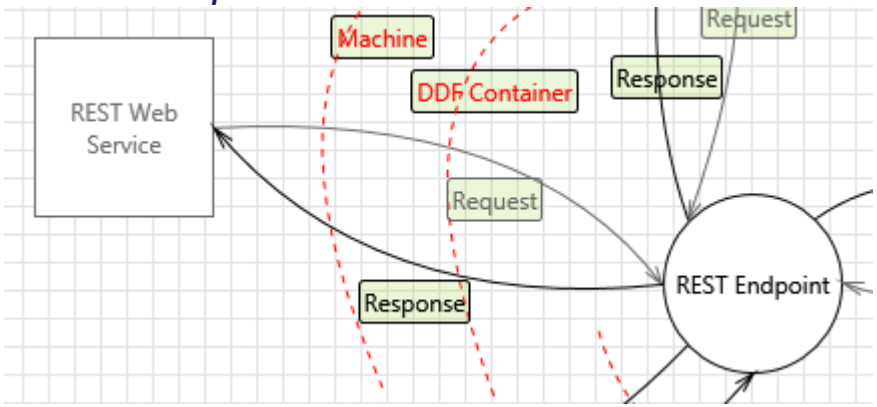
Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.

Justification:	Both the REST Endpoint and DDF Catalog reside within the same application container.

29. REST Endpoint Process Memory Tampered [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	If REST Endpoint is given access to memory, such as shared memory or pointers or is given the ability to control what DDF Catalog executes (for example, passing back a function pointer.), then REST Endpoint can tamper with DDF Catalog. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification:	Memory management is handled by the Java Virtual Machine.

Interaction: Response



30. Spoofing of the REST Web Service External Destination Entity [State: Needs Investigation] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

Description:	REST Web Service may be spoofed by an attacker, and this may lead to data being sent to the attacker's target instead of REST Web Service. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Enable Web Service Security and ensure clients are authenticated prior to accessing the ECDR Endpoints. (ECDR Mitigation #2 – Hardening Checklist)

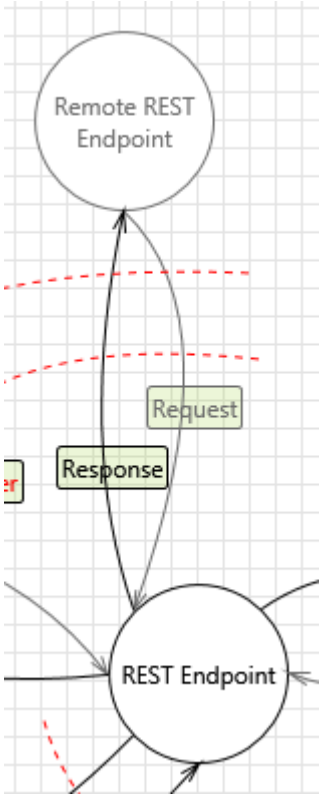
31. External Entity REST Web Service Potentially Denies Receiving Data [State: Needs Investigation] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	REST Web Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time and summary of the received data.
Justification:	Added to ECDR Backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-79

32. Data Flow HTTP Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	This threat is mitigated by only installing the ECDR on a properly secured system within a properly secured network. This is a generic assumption of all DIB/DDF applications. (ECDR Mitigation #3 – Hardening Checklist)

Interaction: Response



33. Weak Credential Transit [State: Needs Investigation] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.
Description:	Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.
Justification:	Enable Transport Layer Security on the DDF for the ECDR endpoints. (ECDR Mitigation #4 – Hardening Checklist)

34. Elevation by Changing the Execution Flow in REST Endpoint [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	An attacker may pass data into Remote REST Endpoint in order to change the flow of program execution within Remote REST Endpoint to the attacker's choosing.
Justification:	All input to the REST Endpoint is processed by an input validator. Furthermore, all input is fuzz tested piror to release.

35. REST Endpoint May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	REST Endpoint may be able to remotely execute code for Remote REST Endpoint.
Justification:	REST Endpoint performs input validation on all inputs. Additionally, all inputs are fuzz tested prior to release.

36. Data Flow HTTP Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	This is a generic system level threat that is mitigated by installing the ECDR onto a properly secured system within a properly secured network. This is a generic assumption of all DIB/DDF apps. (ECDR Mitigation #3 – Hardening Checklist)

37. Potential Process Crash or Stop for REST Endpoint [State: Not Applicable] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	Remote REST Endpoint crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification:	Remote REST Endpoint is out of scope for this threat model.

38. Data Flow Sniffing [State: Needs Investigation] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.
Description:	Data flowing across Response may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification:	Enable Transport Layer Security on the DDF for the ECDR endpoints. (ECDR Mitigation #4 – Hardening Checklist)

39. Collision Attacks [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.
Justification:	This is a generic system level threat that is mitigated by installing the ECDR onto a properly secured system within a properly secured network. This is a generic assumption of all DIB/DDF apps.

40. Replay Attacks [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.
Justification:	This is a generic system level threat that is mitigated by installing the ECDR onto a properly secured system within a properly secured network. This is a generic assumption of all DIB/DDF apps. (ECDR Mitigation #3 – Hardening Checklist)

41. Potential Data Repudiation by REST Endpoint [State: Needs Investigation] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	Remote REST Endpoint claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time and summary of the received data.
Justification:	Added to ECDR backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-79

42. Potential Lack of Input Validation for REST Endpoint [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Data flowing across Response may be tampered with by an attacker. This may lead to a denial of service attack against Remote REST Endpoint or an elevation of privilege attack against Remote REST Endpoint or an information disclosure by Remote REST Endpoint. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification:	All input to REST Endpoint is processed by an input validator. Furthermore, all inputs are fuzz tested prior to release.

43. Spoofing the REST Endpoint Process [State: Needs Investigation] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	Remote REST Endpoint may be spoofed by an attacker, and this may lead to information disclosure by REST Endpoint. Consider using a standard authentication mechanism to identify the destination process.
Justification:	Enable Transport Layer Security on the DDF for the ECDR endpoints. (ECDR Mitigation #4 – Hardening Checklist)

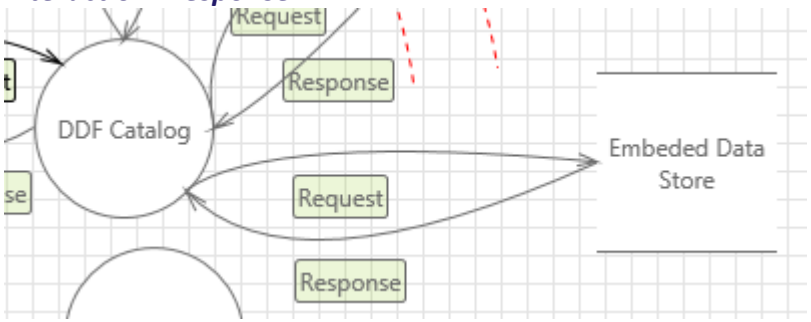
44. Spoofing the REST Endpoint Process [State: Not Applicable] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	REST Endpoint may be spoofed by an attacker, and this may lead to unauthorized access to Remote REST Endpoint. Consider using a standard authentication mechanism to identify the source process.
Justification:	Threats to Remote REST Endpoint are out of scope for this Threat Model.

45. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category:	A user subject gains increased capability or privilege by taking advantage of an implementation bug.
Description:	Remote REST Endpoint may be able to impersonate the context of REST Endpoint in order to gain additional privilege.
Justification:	There is no identifiable scenario in which this is possible or plausible. The Remote REST Endpoint is simply a client application.

Interaction: Response

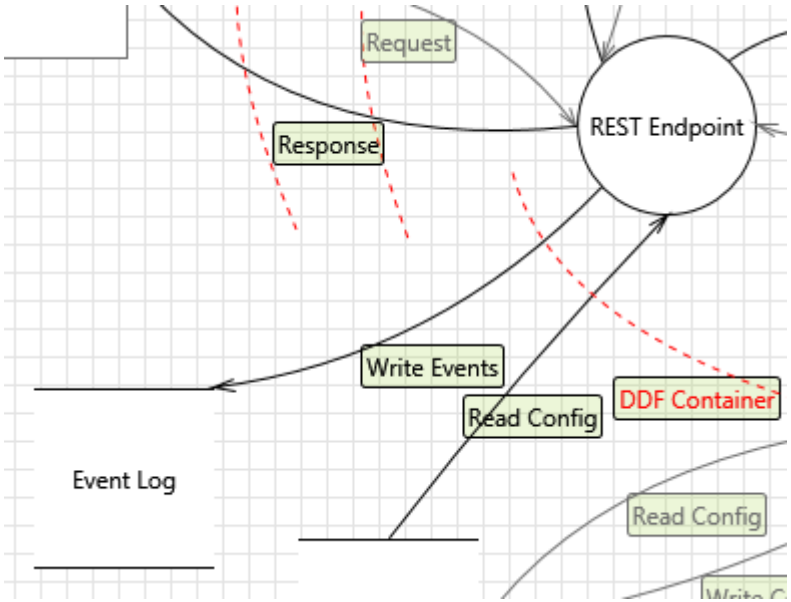


46. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.

Description:	Improper data protection of Embeded Data Store can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification:	Enable Web Service Security and ensure clients are authenticated prior to accessing the ECDR Endpoints. (ECDR Mitigation #2 – Hardening Checklist) Enable Identification and Authentication for embedded data stores. (ECDR Mitigation #5 – Hardening Checklist)

Interaction: Write Events



47. Potential Weak Protections for Audit Data [State: Needs Investigation] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.

Description:	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect
Justification:	May need a DIB/DDF Mitigation

48. Insufficient Auditing [State: Needs Investigation] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert, as well as a privacy expert about your choice of data.
Justification:	Added to ECDR backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-79

49. Data Logs from an Unknown Source [State: Mitigation Implemented] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.
Justification:	Logs are generated by the system/application only.

50. Lower Trusted Subject Updates Logs [State: Mitigation Implemented] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	If you have trust levels, is anyone outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.
Justification:	Logs are only generated by DIB/DDF Apps that run at the same privilege level. Logs are not generated by users.

51. Risks from Logging [State: Not Applicable] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.
Justification:	The ECDR does not provide a log reading capability. The hosting system or DIB/DDF owns the responsibility for this type of threat.

52. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent prevents access to a data store on the other side of the trust boundary.
Justification:	Both reside on the same machine.

53. Data Flow Binary Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	Both reside on the same machine.

54. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category:	Information disclosure happens when the information can be read by an unauthorized party.
Description:	Data flowing across Write Events may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification:	Both reside on the same machine.

55. Data Store Denies Event Log Potentially Writing Data [State: Not Applicable] [Priority: High]

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	Event Log claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time and summary of the received data.
Justification:	Still within the machine trust boundary.

56. The Event Log Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category:	Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with data flow involves changing bits on the wire or between two running processes.
Description:	Data flowing across Write Events may be tampered with by an attacker. This may lead to corruption of Event Log. Ensure the integrity of the data flow to the data store.
Justification:	ECDR and Event Log reside on the same machine.

57. Spoofing the REST Endpoint Process [State: Not Applicable] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	REST Endpoint may be spoofed by an attacker, and this may lead to unauthorized access to Event Log. Consider using a standard authentication mechanism to identify the source process.
Justification:	All DDF apps have access to the logging function. Only an application explicitly installed by the DDF administrator would be able to impersonate the REST Endpoint.

58. Potential Excessive Resource Consumption for REST Endpoint or Event Log [State: Needs Investigation] [Priority: High]

Category:	Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.
Description:	Does REST Endpoint or Event Log take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification:	Added to ECDR Backlog: https://di2e-ecdr.atlassian.net/browse/ECDR-76

59. Spoofing of Destination Data Store Event Log [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description:	Event Log may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of Event Log. Consider using a standard authentication mechanism to identify the destination data store.
Justification:	Spoofing of the Event Log is mitigated by installing the ECDR App on a properly secured system within a properly secured network.

9.2. Controls Trace Matrix

The below table is an enumeration of the security controls and guidance from NIST and DISA as it applies to the ECDR application.

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
AC-10	The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].		X	
AC-11	The information system:		X	
AC-11 (1)	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.		X	

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
AC-12	The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].		X	
AC-12 (1)	The information system:		X	
AC-14	The organization:		X	
AC-16	The organization:		X	
AC-2	The organization:		X	
AC-2 (1)	The organization employs automated mechanisms to support the management of information system accounts.		X	
AC-2 (10)	The information system terminates shared/group account credentials when members leave the group.		X	
AC-2 (11)	The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].		X	
AC-2 (2)	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].		X	
AC-2 (3)	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].		X	
AC-2 (4)	The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].		X	
AC-2 (7)	The organization:		X	
AC-21	The organization:		X	

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.		X	
AC-3 (4)	The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:		X	
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].		X	
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.		X	
AC-6 (10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.		X	
AC-6 (9)	The information system audits the execution of privileged functions.		X	
AC-7	The information system:		X	
AC-8	The information system:		X	
AU-10	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].		X	
AU-12	The information system:		X	
AU-12 (3)	The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].		X	

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
AU-14	The information system provides the capability for authorized users to select a user session to capture/record or view/hear.		X	
AU-14 (2)	The information system provides the capability for authorized users to capture/record and log content related to a user session.		X	
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.		X	
AU-3 (1)	The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].		X	
AU-5 (1)	The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.		X	
AU-5 (2)	The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].		X	
AU-7	The information system provides an audit reduction and report generation capability that:		X	
AU-7 (1)	The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].		X	
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		X	
AU-9 (3)	The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.		X	
CA-2	The organization:	X		

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
CA-2 (1)	The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.			X
CA-2 (2)	The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].			X
CA-5	The organization:			X
CA-8	The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].			
CM-1	The organization:			X
CM-10	The organization:	X		
CM-10 (1)	The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].			X
CM-3	The organization:			X
CM-3 (2)	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.			
CM-3 (4)	The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].	X		
CM-4	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	X		
CM-4 (1)	The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	X		

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
CM-9	The organization develops, documents, and implements a configuration management plan for the information system that:			X
CP-10 (2)	The information system implements transaction recovery for systems that are transaction-based.			X
IA-10	The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].		X	
IA-11	The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].		X	
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).		X	
IA-2 (1)	The information system implements multifactor authentication for network access to privileged accounts.		X	
IA-2 (11)	The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].		X	
IA-2 (12)	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.		X	
IA-2 (2)	The information system implements multifactor authentication for network access to non-privileged accounts.		X	
IA-2 (8)	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.		X	
IA-2 (9)	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.		X	

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
IA-5	The organization manages information system authenticators by:		X	
IA-5 (1)	The information system, for password-based authentication:		X	
IA-5 (11)	The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].		X	
IA-5 (13)	The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].		X	
IA-5 (2)	The information system, for PKI-based authentication:		X	
IA-5 (7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	X		
IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		X	
IA-7	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.		X	
IA-8	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		X	
IA-8 (1)	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.		X	
IA-8 (2)	The information system accepts only FICAM-approved third-party credentials.		X	
IA-8 (3)	The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.		X	
IA-8 (4)	The information system conforms to FICAM-issued profiles.		X	

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
PL-1	The organization:			X
PL-2	The organization:	X		
PL-7	The organization:			X
PL-8	The organization:			X
PM-6	The organization develops, monitors, and reports on the results of information security measures of performance.	X		
RA-1	The organization:	X		
RA-3	The organization:	X		
SA-1	The organization:			X
SA-10	The organization requires the developer of the information system, system component, or information system service to:	X		
SA-10 (1)	The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.		X	
SA-11	The organization requires the developer of the information system, system component, or information system service to:	X		
SA-11 (1)	The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	X		
SA-11 (2)	The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	X		

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SA-11 (4)	The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].	X		
SA-11 (5)	The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [Assignment: organization-defined breadth/depth] and with [Assignment: organization-defined constraints].	X		
SA-11 (6)	The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.	X		
SA-11 (7)	The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [Assignment: organization-defined depth of testing/evaluation].	X		
SA-12	The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	X		
SA-12 (9)	The organization employs [Assignment: organization-defined Operations Security (OPSEC) safeguards] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.	X		
SA-15	The organization:			X
SA-15 (1)	The organization requires the developer of the information system, system component, or information system service to:			X
SA-15 (11)	The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.	X		

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SA-15 (2)	The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.	X		
SA-15 (3)	The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle].			X
SA-15 (4)	The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that:	X		
SA-15 (5)	The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	X		
SA-15 (6)	The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.			X
SA-15 (7)	The organization requires the developer of the information system, system component, or information system service to:	X		
SA-15 (8)	The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.	X		
SA-16	The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.			X
SA-17	The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:			X
SA-17 (1)	The organization requires the developer of the information system, system component, or information system service to:			X

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SA-17 (2)	The organization requires the developer of the information system, system component, or information system service to:			X
SA-17 (3)	The organization requires the developer of the information system, system component, or information system service to:			X
SA-17 (4)	The organization requires the developer of the information system, system component, or information system service to:			X
SA-17 (5)	The organization requires the developer of the information system, system component, or information system service to:			X
SA-17 (6)	The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.			X
SA-17 (7)	The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.		X	
SA-2	The organization:			X
SA-22	The organization:			X
SA-3	The organization:	X		
SA-4	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:			X
SA-4 (1)	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	X		

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SA-4 (10)	The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.		X	
SA-4 (2)	The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].	X		
SA-4 (3)	The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes].	X		
SA-4 (5)	The organization requires the developer of the information system, system component, or information system service to:	X		
SA-4 (9)	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	X		
SA-5	The organization:	X		
SA-8	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	X		
SC-11	The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].			X
SC-13	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.			X

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SC-18	The organization:	X		
SC-18 (2)	The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code requirements].	X		
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	X		
SC-2 (1)	The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.	X		
SC-21	The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.		X	
SC-23	The information system protects the authenticity of communications sessions.		X	
SC-23 (1)	The information system invalidates session identifiers upon user logout or other session termination.		X	
SC-23 (3)	The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session identifiers that are system-generated.		X	
SC-24	The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	X		
SC-28	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].		X	
SC-38	The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.			X

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.			X
SC-8	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.		X	
SC-8 (1)	The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].		X	
SC-8 (2)	The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.		X	
SI-10	The information system checks the validity of [Assignment: organization-defined information inputs].	X		
SI-10 (3)	The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	X		
SI-11	The information system:	X		
SI-16	The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.		X	
SI-2	The organization:	X		
SI-2 (2)	The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.			X
SI-2 (3)	The organization:			X
SI-5	The organization:			X
SI-5 (1)	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.			X

Control	Description	Developer / Software	Hosting Platform	Sponsor / No Capability
SI-7	The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].		X	
SI-7 (14)	The organization:			
SI-7 (15)	The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation.	X		

9.3. Security Test Master Table

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-10	Access Control // Concurrent Session Control		Tested	Session Control is handled by the platform	Pass		X	
AC-10		The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Tested	Session Control is handled by the platform	Pass		X	
AC-11	Access Control // Session Lock		Tested	Session Control is handled by the platform	Pass		X	
AC-11		The information system:	Tested	Session Control is handled by the platform	Pass		X	
AC-11	AC-11a.	Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and	Tested	Session Control is handled by the platform	Pass		X	
AC-11	AC-11b.	Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Tested	Session Control is handled by the platform	Pass		X	
AC-11 (1)	Access Control // Session Lock | Pattern-Hiding Displays		Tested	Session Control is handled by the platform	Pass		X	
AC-11 (1)		The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Tested	Session Control is handled by the platform	Pass		X	
AC-12	Access Control // Session Termination		Tested	Session Control is handled by the platform	Pass		X	
AC-12		The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Tested	Session Control is handled by the platform	Pass		X	
AC-12 (1)	Access Control // Session Termination |User-Initiated Logouts/ Message Displays		Tested	Session Control is handled by the platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-12 (1)		The information system:	Tested	Session Control is handled by the platform	Pass		X	
AC-12 (1)	AC-12 (1)(a)	Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and	Tested	Session Control is handled by the platform	Pass		X	
AC-12 (1)	AC-12 (1)(b)	Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	Tested	Session Control is handled by the platform	Pass		X	
AC-14	Access Control // Permitted Actions Without Identification Or Authentication		Tested	Controlled by DIB WSS or Hosting System	Pass		X	
AC-14		The organization:	Tested	Controlled by DIB WSS or Hosting System	Pass		X	
AC-14	AC-14a.	Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and	Tested	Controlled by DIB WSS or Hosting System	Pass		X	
AC-14	AC-14b.	Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	Tested	Controlled by DIB WSS or Hosting System	Pass		X	
AC-16	Access Control // Security Attributes		Tested	Security labels are handled by DDF Security	Pass		X	
AC-16		The organization:	Tested	Security labels are handled by DDF Security	Pass		X	
AC-16	AC-16a.	Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission;	Tested	Security labels are handled by DDF Security	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-16	AC-16b.	Ensures that the security attribute associations are made and retained with the information;	Tested	Security labels are handled by DDF Security	Pass		X	
AC-16	AC-16c.	Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and	Tested	Security labels are handled by DDF Security	Pass		X	
AC-16	AC-16d.	Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.	Tested	Security labels are handled by DDF Security	Pass		X	
AC-2	Access Control // Account Management		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2		The organization:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2a.	Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2b.	Assigns account managers for information system accounts;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2c.	Establishes conditions for group and role membership;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2d.	Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2e.	Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2f.	Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2g.	Monitors the use of information system accounts;	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-2	AC-2h.	Notifies account managers:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2h.1.	When accounts are no longer required;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2h.2.	When users are terminated or transferred; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2h.3.	When individual information system usage or need-to-know changes;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2i.	Authorizes access to the information system based on:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2i.1.	A valid access authorization;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2i.2.	Intended system usage; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2i.3.	Other attributes as required by the organization or associated missions/business functions;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2j.	Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	AC-2k.	Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2	Access Control // Account Management		Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-2	V-16847	Interview the application representative to verify that a documented process exists for user and system account creation, termination, and expiration. Obtain a list of recently departed personnel and verify that their accounts were removed or deactivated on all systems in a timely manner (e.g., less than two days). 1) If a documented account management process does not exist or unauthorized users have active accounts, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (1)	Access Control // Account Management | Automated System Account Management		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (1)		The organization employs automated mechanisms to support the management of information system accounts.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (10)	Access Control // Account Management | Shared/ Group Account Credential Termination		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (10)		The information system terminates shared/group account credentials when members leave the group.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (11)	Access Control // Account Management | Usage Conditions		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (11)		The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (2)	Access Control // Account Management | Removal of Temporary/ Emergency Accounts		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (2)		The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (3)	Access Control // Account Management | Disable Inactive Accounts		Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-2 (3)		The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (4)	Access Control // Account Management | Automated Audit Actions		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (4)		The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (7)	Access Control // Account Management | Role-Based Schemes		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (7)		The organization:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (7)	AC-2 (7)(a)	Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (7)	AC-2 (7)(b)	Monitors privileged role assignments; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-2 (7)	AC-2 (7)(c)	Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-21	Access Control // Information Sharing		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-21		The organization:	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-21	AC-21a.	Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-21	AC-21b.	Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	Access Control // Access Enforcement		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3		The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	V-16789	Interview the application representative and determine the keys resident on application servers (including X.509 certificates). For the purposes of this checklist, no more than 20 keys need to be examined. Based on the number of keys in the inventory, determine if all of the keys will be examined, or just a sample. If a sample will be selected, choose keys of a variety of types (certificate of a certificate authority, certificate of a user, private key of a user, etc.). No user or process should be able to write to any file containing keys. If keys need to be replaced or added, permissions can be changed temporarily for those events. 1) If any privileged or non-privileged user or application process has write permissions to a file containing cryptographic keys, it is a finding. Determine if when keys are read, that transaction occurs under the security context of a user account, or of the application process (which would perform the transaction on behalf of the user). Ensure that read permissions are granted only to the account(s) that must know the key to make the application function. If any user groups are granted read permissions, check that the members of these groups contain only the users that require knowledge of the key. 2) If any user accounts have read (or greater) permissions to a private or secret key, which do not require such permissions, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		3) If any group with read permissions contains a user that does not require such permissions, it is a finding.						
AC-3	V-16798	Identification and authentication information must be protected by appropriate file permissions. Only administrators and the application or OS process that access the information should have any permissions to access identification and authentication information. In many cases, local backups of the accounts database exist so these must be included in the scope of the review. 1) If non-privileged users have the permission to read or write password files, other than resetting their own password, this is a CAT II finding. 2) If non-privileged users can read user information (e.g., list users but not passwords), this is a CAT III finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	V-16803	Ask the application representative to demonstrate the application resources have appropriate access permissions. 1) If the application representative cannot demonstrate all application resources have appropriate access permissions, it is a finding. Review the locations of all configuration files used by the application. Ask the application representative to demonstrate configuration files used by the application are restricted to authorized users. 2) If access permissions to configuration files are not restricted to application administrators, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	V-16814	Ask the application representative to demonstrate the application does not disclose any information about the application which could be used by an attacker to gain access to the application. UDDI registries should also not provide any information about the application which could be used by an attacker to gain access to the web service. WSDL should not provide unnecessary information (especially debugging features). Ask the application representative to login as a non-privileged user and review all screens of the application to identify any potential data that should not be disclosed to the user.	Tested	Reviewed through HP Fortify	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		1) If the application displays any data that should not be disclosed, this is a finding.						
AC-3	V-16816	Ask the application representative to login as an unprivileged user and demonstrate the application creates transaction logs for access and changes to the data. Verify transaction logs exist and the log records access and changes to the data. This check is in addition to the ECAR auditing requirements. 1) If the application representative cannot demonstrate the above, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	V-16818	Ask the application representative to demonstrate how the application provides the users of time and date of the last change in data content. This may be demonstrated in application logs, audit logs, or database tables and logs. 1) If the application representative cannot demonstrate the above, this is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3	V-16841	Interview application representative and ask for the system documentation that states how often audit logs are reviewed. Also, determine when the audit logs were last reviewed. 1) If the application representative cannot provide system documentation identifying how often the auditing logs are reviewed, or has not audited within the last time period stated in the system documentation, it is a finding.	Tested	Hosting Environment is outside the scope of this evaluation	NA			X
AC-3	V-6141	Policy: The designer will ensure access control mechanisms exist to ensure data is accessed and changed only by authorized personnel. The designer will ensure the access procedures enforce the principles of separation of duties and "least privilege." The IAO will ensure the access procedures enforce the principles of separation of duties and "least privilege." Ask the application representative if particular administrative and user functions can be restricted to certain roles. The objective is to ensure that the application prohibits combination of roles that represent an IA risk. In particular, inquire about separation of duties between the following: • Personnel that review and clear audit logs and personnel that perform non-audit administration. • Personnel that create, modify, and delete access control rules and personnel that perform either	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		data entry or application programming. Some applications may only contain administrator access and no other access. For example, network appliances may have administrator only access. Web applications with no user authentication required are also considered to contain a single role, unless the web application provides administrative access to publish web server content. 1) If the application is designed specifically to only have one role, this check is not applicable. 2) If the application representative states that the application does not enforce separation of duties between the roles listed above, it is a finding. If the representative claims that the required separation exists, identify which software component is enforcing it. Evidence of enforcement can either involve the display of relevant security configuration settings or a demonstration using different user accounts, each assigned to a different role. 3) If the application representative cannot provide evidence of separation of duties, it is a finding. *Note: Web services are required to implement role-based access control.						
AC-3 (4)	Access Control // Access Enforcement | Discretionary Access Control		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3 (4)		The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3 (4)	AC-3 (4)(a)	Pass the information to any other subjects or objects;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3 (4)	AC-3	Grant its privileges to other subjects;	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
	(4)(b)							
AC-3 (4)	AC-3 (4)(c)	Change security attributes on subjects, objects, the information system, or the information system's components;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3 (4)	AC-3 (4)(d)	Choose the security attributes to be associated with newly created or revised objects; or	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-3 (4)	AC-3 (4)(e)	Change the rules governing access control.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-4	Access Control // Information Flow Enforcement		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-4		The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-6	Access Control // Least Privilege		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-6		The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-6 (10)	Access Control // Least Privilege | Prohibit Nonprivileged Users from Executing Privileged Functions		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-6 (10)		The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-6 (9)	Access Control // Least Privilege | Auditing Use of Privileged Functions		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-6 (9)		The information system audits the execution of privileged functions.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	Access Control // Unsuccessful Login Attempts		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7		The information system:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	AC-7a.	Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	AC-7b.	Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	Access Control // Unsuccessful Login Attempts		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	V-16800	Ask the application representative to demonstrate the application locks a user account if a user enters a password incorrectly more than three times in a 60 minute period. 1) If the account is not disabled, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	V-16801	Ask the application representative to demonstrate that only the administrator can unlock locked accounts. 1) If the application allows non-administrator to unlock accounts, it is a finding.	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-7	V-16802	Interview application representative to identify the length of time a user can be idle before the application will time out and terminate the session and require reauthentication. 1) If the application representative states that one or all of the limits are absent for one or more	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		session types, it is a finding. In many cases, session configuration parameters can be examined. If configuration parameters are embedded within the application they may not be available for review. Any configuration settings that are not configurable should be manually tested. The preferred method depends on the application environment. Manually validate session limits by empirical testing (logon on multiple times and leaving sessions idle). In some cases, testing session limits is not feasible because they may be set too high to properly simulate them during the review. Even if the application does not provide time limits for idle sessions, such limits may exist at the transport layer (e.g., TCP timeouts). Consider all possible ways in which limits might be enforced before documenting a finding. 2) If there is no evidence of a required session timeout, it is a finding.						
AC-7	V-16817	Policy: The designer will ensure the application has a capability to notify the user on logon of date and time of the user's last unsuccessful logon, IP address of the user's last unsuccessful logon, date and time of the user's last successful logon, IP address of the user's last successful logon, and number of unsuccessful logon attempts since the last successful logon. Check: If the application uses password authentication, try to logon to the system using an incorrect password. Restart the application and logon again using the correct password. After a successful logon to the application, logout of the application and note the date and times for the last success and unsuccessful logons. Again, logon to the application and determine whether the application correctly displays the following information immediately at logon: Unsuccessful Logon Date	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Time IP Address Successful Logon Date Time IP Address If the application does not correctly display the last unsuccessful and successful logon information immediately at login, it is a finding For CAC and NSA approved token authentication logons, remove the CAC or mistype the PIN to simulate an unsuccessful login.						
AC-7	V-6144	Work with the application representative to identify application modules that involve user or process sessions (e.g., a user may initiate a session with a web server, which in turn maintains sessions with a backend database server). For each session type, ask the application representative the limits on: • Number of sessions per user ID • Number of sessions per application 1) If the application representative states the session limits are absent for any of the session types, it is a finding. In many cases, session configuration parameters can be examined. If configuration parameters are embedded within the application, they may not be available for review. Any configuration settings that are not configurable should be manually tested. The preferred method depends on the application environment. 2) If there is no evidence of a required session limit on one or more of the session types, it is a finding. The finding details should note specifically which types of sessions are left unbounded, and thus, more vulnerable to DoS attacks.	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-8	Access Control // System Use Notification		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8		The information system:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8a.	Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8a.1.	Users are accessing a U.S. Government information system;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8a.2.	Information system usage may be monitored, recorded, and subject to audit;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8a.3.	Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8a.4.	Use of the information system indicates consent to monitoring and recording;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8b.	Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8c.	For publicly accessible systems:	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8c.1.	Displays system use information [Assignment: organization-defined conditions], before granting further access;	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8c.2.	Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and	Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	AC-8c.3.	Includes a description of the authorized uses of the system.	Tested	Account Management is handled by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AC-8	Access Control // System Use Notification		Tested	Account Management is handled by the hosting platform	Pass		X	
AC-8	V-6152	Logon to the application. If a warning message appears, compare it to the two following banners: (Use the following banner for desktops, laptops, and other devices accommodating banners of 1300 characters) You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. (For Blackberries and other PDAs/PEDs with severe character limitations use the following banner): I've read & consent to terms in IS user agreem't.	Tested	There is no UI for ECDR	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		These banners are mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance. 1) If the login banner is not one of the above banners or the login banner is missing this is a finding. If the only way to access the application is through the OS, then an additional banner is not required at the application level.						
AU-10	Audit and Accountability // Non-Repudiation		Tested	DDF Security handles auditing	Pass		X	
AU-10		The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].	Tested	DDF Security handles auditing	Pass		X	
AU-12	Audit and Accountability // Audit Generation		Tested	DDF Security handles auditing	Pass		X	
AU-12		The information system:	Tested	DDF Security handles auditing	Pass		X	
AU-12	AU-12a.	Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];	Tested	DDF Security handles auditing	Pass		X	
AU-12	AU-12b.	Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and	Tested	DDF Security handles auditing	Pass		X	
AU-12	AU-12c.	Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	Tested	DDF Security handles auditing	Pass		X	
AU-12 (3)	Audit and Accountability // Audit Generation | Changes by Authorized Individuals		Tested	DDF Security handles auditing	Pass		X	
AU-12 (3)		The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	Tested	DDF Security handles auditing	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
AU-14	Audit and Accountability // Session Audit		Tested	Audit reduction and review is provided by the hosting system	Pass		X	
AU-14		The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	Tested	Audit reduction and review is provided by the hosting system	Pass		X	
AU-14 (2)	Audit and Accountability // Session Audit | Capture/Record and Log Content		Tested	Audit reduction and review is provided by the hosting system	Pass		X	
AU-14 (2)		The information system provides the capability for authorized users to capture/record and log content related to a user session.	Tested	Audit reduction and review is provided by the hosting system	Pass		X	
AU-3	Audit and Accountability // Content Of Audit Records		Tested	DDF Security handles auditing	Pass		X	
AU-3		The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Tested	DDF Security handles auditing	Pass		X	
AU-3 (1)	Audit and Accountability // Content Of Audit Records| Additional Audit Information		Tested	DDF Security handles auditing	Pass		X	
AU-3 (1)		The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].	Tested	DDF Security handles auditing	Pass		X	
AU-5 (1)	Audit and Accountability // Response To Audit Processing Failures | Audit Storage Capacity		Tested	Account Management is provided by the hosting platform	Pass		X	
AU-5 (1)		The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.	Tested	Account Management is provided by the hosting platform	Pass		X	
AU-5 (2)	Audit and Accountability // Response To Audit Processing Failures | Real-Time Alerts		Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-5 (2)		The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit	Tested	Audit Management is provided by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].						
AU-7	Audit and Accountability // Audit Reduction And Report Generation		Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-7		The information system provides an audit reduction and report generation capability that:	Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-7	AU-7a.	Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and	Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-7	AU-7b.	Does not alter the original content or time ordering of audit records.	Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-7 (1)	Audit and Accountability // Audit Reduction And Report Generation | Automatic Processing		Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-7 (1)		The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-9	Audit and Accountability // Protection Of Audit Information		Tested	Audit Management is provided by the hosting platform	Fail		X	
AU-9		The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Tested	Audit Management is provided by the hosting platform	Fail		X	
AU-9	V-6140	Locate the application audit log location. Examine the properties of the log files. For a Windows system, the NTFS file permissions should be System – Full control, Administrators and Application Administrators - Read, and Auditors - Full Control. 1) If the log files have permissions more permissive than what is listed, it is a finding. For UNIX systems, use the ls –la (or equivalent) command to check the permissions of the audit log files.	Tested	Audit Management is provided by the hosting platform	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If excessive permissions exist, it is a finding.						
AU-9 (3)	Audit and Accountability // Protection Of Audit Information | Cryptographic Protection		Tested	Audit Management is provided by the hosting platform	Pass		X	
AU-9 (3)		The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	Tested	Audit Management is provided by the hosting platform	Pass		X	
CA-2	Security Assessment and Authorization // Security Assessments		Tested		Pass	X		
CA-2		The organization:	Tested		Pass	X		
CA-2	CA-2a.	Develops a security assessment plan that describes the scope of the assessment including:	Tested		Pass	X		
CA-2	CA-2a.1.	Security controls and control enhancements under assessment;	Tested		Pass	X		
CA-2	CA-2a.2.	Assessment procedures to be used to determine security control effectiveness; and	Tested		Pass	X		
CA-2	CA-2a.3.	Assessment environment, assessment team, and assessment roles and responsibilities;	Tested		Pass	X		
CA-2	CA-2b.	Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;	Tested		Pass	X		
CA-2	CA-2c.	Produces a security assessment report that documents the results of the assessment; and	Tested		Pass	X		
CA-2	CA-2d.	Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
CA-2 (1)	Security Assessment and Authorization // Security Assessments | Independent Assessors		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-2 (1)		The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-2 (2)	Security Assessment and Authorization // Security Assessments | Specialized Assessments		Tested	Hosting Environment is outside the scope of this evaluation	NA			X
CA-2 (2)		The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].	Tested	Hosting Environment is outside the scope of this evaluation	NA			X
CA-5	Security Assessment and Authorization // Plan Of Action And Milestones		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-5		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-5	CA-5a.	Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-5	CA-5b.	Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CA-8	Security Assessment and Authorization // Penetration Testing		Tested		Pass			
CA-8		The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].	Tested		Pass			
CM-1	Configuration Management // Configuration Management Policy And Procedures		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
CM-1		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1a.	Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1a.1.	A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1a.2.	Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1b.	Reviews and updates the current:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1b.1.	Configuration management policy [Assignment: organization-defined frequency]; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	CM-1b.2.	Configuration management procedures [Assignment: organization-defined frequency].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-1	Configuration Management // Configuration Management Policy And Procedures		Tested	No developer level CM plan exists	Failed			X
CM-1	V-16822	The Release Manager will ensure the SCM plan identifies all objects created during the development process subject to configuration control. The Release Manager will ensure the SCM plan maintains procedures for identifying individual application components, as well as, entire application releases during all phases of the software development lifecycle. The Release Manager will ensure the SCM plan identifies and tracks all actions and changes resulting from a change request from initiation to release. The Release Manager will ensure the SCM plan contains procedures to identify, document, review, and authorize any change requests to the application.	Tested	No developer level CM plan exists	Failed			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The Release Manager will ensure the SCM plan defines the responsibilities, the actions to be performed, the tools, techniques and methodologies, and defines an initial set of baselined software components. The Release Manager will ensure the SCM plan objects have security classifications labels. The Release Manager will ensure the SCM plan identifies tools and version numbers used in the software development lifecycle. The Release Manager will ensure the SCM plan identifies mechanisms for controlled access of simultaneous individuals updating the same application component. The Release Manager will ensure the SCM plan assures only authorized changes by authorized persons are possible. The Release Manager will ensure the SCM plan identifies mechanisms to control access and audit changes between different versions of objects subject to configuration control. The Release Manager will ensure the SCM plan identifies mechanisms to track and audit all modifications of objects under configuration control. Audits will include the originator and date and time of the modification. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Ask the application representative to review the applications SCM plan. The SCM plan should contain the following: • Description of the configuration control and change management process • Types of objects developed • Roles and responsibilities of the organization 1) If the SCM plan does not include the above, this is a CAT II finding.						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The SCM plan should also contain the following: • Defined responsibilities • Actions to be performed • Tools used in the process • Techniques and methodologies • Initial set of baselined software components 2) If the SCM plan does not include the above, this is a CAT III finding. The SCM plan should identify all objects that are under configuration management control. Ask the application representative to provide access to the configuration management repository and to identify the objects shown in the SCM plan. 3) If the application representative cannot display all types of objects under CM control, this is a CAT III finding. The SCM plan should identify third party tools and respective version numbers. 4) If the SCM plan does not identify third party tools, this is a CAT II finding. The SCM plan should identify mechanisms for controlled access of individuals simultaneously updating the same application component. 5) If the SCM plan does not identify mechanisms for controlled access, this is a CAT III finding. The SCM plan assures only authorized changes by authorized persons are allowed. 6) If the SCM plan does not assure only authorized changes are made, this is a CAT II finding. The SCM plan should identify mechanisms to control access and audit changes between different versions of objects subject to configuration control. 7) If the SCM plan does not identify mechanisms to control access and to audit changes between different versions of objects subject to configuration control, this is a CAT III finding.						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The SCM plan should have procedures for label versions of application components and application builds under configuration management control. Ask the application representative demonstrate the configuration management repository and contains versions and releases of the application. Ask the application representative to create a build or demonstrate a current release of the application can be recreated. 8) If the application representative cannot display releases and application component versions, this is a CAT II finding. The configuration management repository should track change requests from beginning to end. Ask the application representative to display a completed or in-process change request. 9) If the configuration management repository cannot tracks change requests, this is a CAT III finding. If the application has just completed its first release, there may not be any change requests logged in the configuration management repository. In this case, this finding is not applicable. The configuration management repository should authorize change requests to the application. Ask the application representative to display an authorized change request and identify who is responsible for authorizing change requests. 10) If the configuration management repository does not track authorized change requests, this is a CAT III finding. If the application has just completed its first release, there may not be any change requests logged in the configuration management repository. In this case, this finding is not applicable. The configuration management repository should contain security classification labels for code and documentation in the repository. Classification labels are not applicable to unclassified systems.							

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		11) If there are no classification labels of code and documentation in the configuration management repository, this is a CAT III finding. The configuration management repository should monitor all objects under CM control for auditing. 12) If the configuration management repository does not audit for modifications, this is a CAT II finding. The SCM plan should identify all components required to be IPV6 capable. 13) If the SCM plan does not identify application components as IPV6 capable, this is a CAT III finding.						
CM-10	Configuration Management // Software Usage Restrictions		Tested		Pass	X		
CM-10		The organization:	Tested		Pass	X		
CM-10	CM-10a.	Uses software and associated documentation in accordance with contract agreements and copyright laws;	Tested		Pass	X		
CM-10	CM-10b.	Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and	Tested		Pass	X		
CM-10	CM-10c.	Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
CM-10 (1)	Configuration Management // Software Usage Restrictions | Open Source Software		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-10 (1)		The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	Configuration Management // Configuration Change Control		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3a.	Determines the types of changes to the information system that are configuration-controlled;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3b.	Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3c.	Documents configuration change decisions associated with the information system;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3d.	Implements approved configuration-controlled changes to the information system;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3e.	Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3f.	Audits and reviews activities associated with configuration-controlled changes to the information system; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	CM-3g.	Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3	Configuration Management // Configuration Change Control		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
CM-3	V-16823	Interview the application representative and determine if a CCB exists. Ask about the membership of the CCB, and identify the primary members. Ask if there is a CCB charter documentation. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If there is no evidence of CCB, it is a CAT II finding. 2) If the IAM is not part of the CCB, it is a CAT II finding. Interview the application representative and determine how often the CCB meets. Ask if there is CCB charter documentation. The CCB charter documentation should indicate how often the CCB meets. If there is no charter documentation, ask when the last time the CCB met and when was the last release of the application. CCB's do not have to physically meet, and the CCB chair may authorize a release based on phone and/or e-mail conversations. 3) If there is not evidence of a CCB meeting during every release cycle, this a CAT III finding.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
CM-3 (2)	Configuration Management // Configuration Change Control | Test/ Validate/ Document Changes		Tested	Operational environment is out of scope of this review	NA	X		
CM-3 (2)		The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	Tested	Operational environment is out of scope of this review	NA			
CM-3 (4)	Configuration Management // Configuration Change Control | Security Representative		Tested	Bobby King is the Security Engineer who reviews and tests the application prior to release	Pass	X		
CM-3 (4)		The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].	Tested	Bobby King is the Security Engineer who reviews and tests the application prior to release	Pass	X		
CM-4	Configuration Management // Security Impact Analysis		Tested	Bobby King is the Security Engineer who reviews and tests the application prior to release	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
CM-4		The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Tested	Bobby King is the Security Engineer who reviews and tests the application prior to release	Pass	X		
CM-4	Configuration Management // Security Impact Analysis		Tested		Pass	X		
CM-4	V-16781	The Program Manager will: - Ensure users are provided with a means of obtaining updates for the application. - Ensure a mechanism is in place to notify users of security flaws, and to provide users with the availability of patches. - Ensure a comprehensive vulnerability management process, including systematic identification and mitigation of software vulnerabilities, is in place. Interview the application representative to determine if users are provided with a means of obtaining updates for the application. 1) If users are not provided with a means of obtaining updates for the application, it is a finding. 2) If updates are transmitted over a LAN, and is not IPv6 capable, it is a finding. Interview the application representative to determine if users are provided a mechanism to be notified of security flaws and the availability of patches. 3) If users are not provided security flaw and patch notifications for the application, it is a finding. 4) If security flaws and patch notifications are transmitted over a LAN, and is not IPv6 capable, it is a finding. Interview the application representative and determine if a vulnerability management process exists. 5) If no vulnerability management process or policy exists, it is a finding. Interview the application representative to determine maintenance is available for production applications.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		6) If maintenance is not available for an application, it is a finding.						
CM-4	V-16825	Interview the application representative and determine if changes to the application are assessed for IA impact prior to implementation. Review the CCB process documentation to ensure potential changes to the application are evaluated to determine impact. An informal group may be tasked with impact assessment of upcoming version changes. 1) If impact analysis is not performed, it is a finding.	Tested	SAT	Pass	X		
CM-4	V-16826	Ask the application representative to provide tests plans, procedures, and results to ensure they are updated for each application release or updates to system patches. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If test plans, procedures, and results do not exist or are not updated for each application release or updates to system patches, this is a finding.	Tested	SAT	Pass	X		
CM-4	V-16835	Review the components of the application. Deployment personnel should be registered to receive updates to all components of the application, such as Web Server, Application Servers, and Database Servers. Also, if update notifications are provided to any custom developed software, deployment personnel should also register for these updates. Ask the application representative to demonstrate deployment personnel are registered to receive notifications for updates to all the application components including and custom developed software. 1) If the application provides automated alerts for update notifications, and no deployment personnel are registered to receive the alerts, it is a finding.	Tested	Sponsor	Sponsor			X
CM-4	V-16836	Ask the application representative to review the Configuration Management Plan. Ensure procedures exist addressing the test and implementation process for all patches, upgrades, and application deployments. Verify all IPv6 applicable patches have been applied. Verify all vendor provided IPv6 related patches been installed. 1) If required patches are missing, it is a finding.	Tested	This level of patch management is intended for the hosting environment and not the code base.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If procedures do not exist or are deficient, it is a finding.						
CM-4 (1)	Configuration Management // Security Impact Analysis | Separate Test Environments		Tested	Operational Environment is out of scope of this review	Sponsor	X		
CM-4 (1)		The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Tested	Operational Environment is out of scope of this review	Sponsor	X		
CM-9	Configuration Management // Configuration Management Plan		Tested	No developer level CM plan exists	Failed			X
CM-9		The organization develops, documents, and implements a configuration management plan for the information system that:	Tested	No developer level CM plan exists	Failed			X
CM-9	CM-9a.	Addresses roles, responsibilities, and configuration management processes and procedures;	Tested	No developer level CM plan exists	Failed			X
CM-9	CM-9b.	Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;	Tested	No developer level CM plan exists	Failed			X
CM-9	CM-9c.	Defines the configuration items for the information system and places the configuration items under configuration management; and	Tested	No developer level CM plan exists	Failed			X
CM-9	CM-9d.	Protects the configuration management plan from unauthorized disclosure and modification.	Tested	No developer level CM plan exists	Failed			X
CP-10 (2)	Contingency Planning // Information System Recovery And Reconstitution | Transaction Recovery		Tested	ECDR is not a database and is not transaction based	NA			X
CP-10 (2)		The information system implements transaction recovery for systems that are transaction-based.	Tested	ECDR is not a database and is not transaction based	NA			X
IA-10	Identification and Authentication // Adaptive Identification and Authentication		Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-10		The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	Tested		Pass		X	
IA-11	Identification and Authentication // Re-authentication		Tested		Pass		X	
IA-11		The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Tested		Pass		X	
IA-2	Identification and Authentication // Identification And Authentication (Organizational Users)		Tested		Pass		X	
IA-2		The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Tested		Pass		X	
IA-2	Identification and Authentication // Identification And Authentication (Organizational Users)		Tested		Pass			
IA-2	V-16795	Ask the application representative to login to the application. If the application uses password authentication, the password should not be displayed as clear text. 1) If the password is displayed as clear text, this is a finding.	Tested	IDAM is provided by a lower level application	NA			X
IA-2	V-16797	With respect to identification and authentication information, only administrators and the application or OS process that access the information should have any permissions to these files. In many cases, local backups of the accounts database exist so these must be included in the scope of the review. Authentication credentials such as passwords are required to be encrypted. Check the configuration of the application software to determine if encryption settings have been activated for the relevant data. 1) If these encryption settings have not been turned on, this is a CAT II finding. If the data encryption functionality is not configurable and the identification and authentication information is stored in ASCII or another readable format, examine the actual data to determine if they are in clear text.	Tested	ECDR does not have permissions to the LDAP/IDAM solution used by the hosting environment	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If the authentication data is readable, this is a CAT I finding. Record findings, regardless of whether or not the vulnerability has been captured in another SRR. For example, any weakness in OS authentication scheme that the application leverages applies both to the OS and the application.						
IA-2	V-16799	Ask the application representative what system accounts are installed/created and/or enabled by default upon installation of the application. 1) If the application installs/creates/enables accounts that are not needed in order for the application to operate, it is a finding.	Tested	No accounts are installed, created, or enabled for ECDR.	NA			X
IA-2	V-16848	Ask the application representative to examine the organization's password policy. 1) If non-human/service accounts are used and are not included in the password policy, it is a finding. 2) If non-human/service accounts policy does not require these accounts to change yearly or when someone with access to the password leaves the duty assignment, it is a finding. The configuration interface may not reveal information related to all the required elements. If this is the case, attempt to violate each element to determine if the policy is enforced. For example, attempt to change a password to one that does not meet the requirements. 3) If there are any shortcomings in the password policy or the configured behavior of any user account, it is a finding. The finding details should note which user accounts are impacted, which of the password parameters are deficient, the current values of these parameters, and the relevant required values. Also, ask the application representative to generate two user account passwords. 4) If there is a recognizable pattern in password generation, it is a finding.	Tested	Hosting Environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-2	V-19702	Examine the contents of a SOAP message using WS Security, all messages should contain timestamps, sequence numbers, and expiration. 1) If messages using WS Security do not contain timestamps, sequence numbers, and an expiration, it is a finding.	Tested	ECDR does not use SOAP	NA			X
IA-2	V-19703	Ask the application representative for the design document. Review the design document for web services. Review the design document and verify validity periods are checked on all messages using WS-Security or SAML assertions. 1) If the design document does not exist, or does not indicate validity periods are checked on messages using WS-Security or SAML assertions, it is a finding.	Tested	The App Container handles all WSS components	NA			X
IA-2	V-19704	If the application does not utilize SAML, this check is not applicable. Ask the application representative for the design document. Review the design document for web services using SAML assertions. Review the design document and verify SAML assertion identifiers are not reused by a single asserting party. 1) If the design document does exist, or does not indicate SAML assertion identifiers which are unique for each asserting party, it is a finding.	Tested	ECDR does not use SAML	NA			X
IA-2	V-19705	If the application does not utilize WS-Security tokens, this check is not applicable. Ask the application representative for the design document. Review the design document for web services using WS-Security tokens. Review the design document and verify all WS-Security tokens are only transmitted after both receiving and sending services have been mutually PKI authenticated. 1) If the design document does not exist, or does not indicate all WS-Security tokens are only transmitted after both receiving and sending services have been mutually PKI authenticated, it is a finding.	Tested	The App Container handles all WSS components	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-2	V-6130	Policy: The designer will ensure the application has the capability to require account passwords having a minimum of 15 alphanumeric characters in length. The designer will ensure the application has the capability to require account passwords contain a mix of upper case letters, lower case letters, numbers, and special characters. The Designer will ensure the application has the capability to require account passwords be changed every 60 days or more frequently. The Designer will ensure passwords do not contain personal information such as names, telephone numbers, account names, birthdates, or dictionary words. The Designer will ensure the application has the capability to limit reuse of account passwords within the last 10 password changes. The Designer will ensure the application has the capability to limit user changes to their account passwords once every 24 hours with the exception of privileged or administrative users. The Designer will ensure the application has the capability to require new account passwords differ from the previous password by at least four characters when a password is changed. The IAO will configure the application to ensure account passwords conform to DoD password policy. If the entire authentication process for the application is performed by the operating system (such is the case for a Desktop Application), this check is Not Applicable. First, inventory all the password based authentication processes present in the application. For example, a web server may effectively act as a client when authenticating with a back-end database server. Peer-to-peer processes also are included because each peer still acts in the role of a client or server for particular transactions. Each process must be evaluated separately. If multiple processes must be used for a single authentication attempt, the combination of the processes should be evaluated to ensure this check is fully met. In addition, the authentication may involve a user account database specific to the application or it may involve leveraging the authentication service of an operating system or directory service. 1) If the authentication process involves the presentation of a user account name only, this is a finding. If the authentication is based on passwords, the passwords must have the following characteristics: • A minimum of 15 characters • Include at least one uppercase alphabetic character	Tested	ECDR does not directly use IDAM	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		• Include at least one lowercase alphabetic character • Include at least one non-alphanumeric (special) character • Expire after 60 days • Be different from the previous 10 passwords used • Be changeable by the administrator at any time • Be changeable by the associated user only once in a 24 hour period (for human user accounts) • Not be changeable by users other than the administrator or the user with which the password is associated • Not contain personal information such as names, telephone numbers, account names, birthdates or dictionary words. 2) If the passwords do not have these characteristics, it is a finding. To verify compliance with these requirements, check the configuration of the software that manages the authentication process (e.g., OS, directory, and database or application software) and determine if each of the criteria listed are met. Also sample individual accounts to determine if any of the policy settings are overridden (e.g., password set to never expire). Focus on non-human user accounts, as these are the most likely to violate the stated requirements. Non-human accounts, sometimes known as services accounts, may not be set to expire after 60 days.						
IA-2	V-6131	If the user accounts used in the application are only operating system or database accounts, this check is Not Applicable. Identify duplicate userids. If these are not available, sort the list by the user name and, if applicable, associated ID number so that duplicates will be contiguous and thus easier to locate. 1) If any duplicates user accounts are discovered, it is a finding. The finding details should specify the duplicates by name, unless they are too numerous to document, in which case a numerical count of the IDs is more appropriate.	Tested	ECDR does not directly use IDAM	NA			X
IA-2	V-6132	If the user accounts used in the application are only operating system or database accounts this check is Not Applicable. Identify all users that have not authenticated in the past 35 days.	Tested	ECDR does not directly use IDAM	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		1) If any of these accounts are enabled, it is a finding.						
IA-2	V-6133	If the user accounts used in the application are only operating system or database accounts, this check is Not Applicable. Built-in accounts are those that are added as part of the installation of the application software. These accounts exist for many common commercial off-the-shelf (COTS) or open source components of enterprise applications (e.g., OS, web browser or database software). If SRRs are performed for these components, this is not applicable because the other SRRs will capture the relevant information and findings. If not, read the installation documentation to identify the built-in accounts. Also peruse the account list for obvious examples (e.g., accounts with vendor names such as Oracle or Tivoli). Verify that these accounts have been removed or disabled. If enabled built-in accounts are present, ask the application representative the reason for their existence. 1) If these accounts are not necessary to run the application, it is a finding. 2) If any of these accounts are privileged, it is a finding.	Tested	ECDR does not directly use IDAM	NA			X
IA-2	V-6134	Run a password-cracking tool, if available, on a copy of each account database (there may be more than one in the application infrastructure). 1) If the password-cracking tool is able to crack the password of a privileged user, this is a CAT I finding. 2) If the password-cracking tool is able to crack the password of a non-privileged user, this is a CAT II finding. Manually attempt to authenticate with the published default password for that account, if such a default password exists. 3) If any privileged built-in account uses a default password – no matter how complex – this is a CAT I finding. 4) If a non-privileged account has a default password, this is a CAT II finding.	Tested	ECDR has no database.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-2	V-6153	Persistent cookies are the primary means by which an application stores authentication information over more than one browser session. If the application is a web-based application, verify that Internet Explorer (IE) is set to warn the user before accepting a cookie. Logon to the application and perform several standard operations, noting if the application ever prompts the user to accept a cookie. Log out, close the browser and check the /Windows/cookies, /Windows/profiles/xyz/cookies, and the /documents and settings/xyz/cookies directories (where xyz is replaced by the Windows user profile name). If a cookie has been placed in either of these directories, open it (using Notepad or another text editor) and search for identification or authentication data that remain after to check for sensitive application data. 1) If authentication credentials exist (e.g., a password), this is a CAT I finding. 2) If identification information (e.g., user name, ID, or key properties) exists, but is not accompanied by authentication credentials such as a password, this is a CAT II finding. The application may use means other than cookies to store user information. If the reviewer detects an alternative mechanism for storing I&A information locally, examine the credentials found. 3) If authentication data (e.g., a password) is found, this is a CAT I finding. 4) If identification information is found (e.g., user name, ID, or key properties) but is not accompanied by authentication credentials such as a password, this is a CAT II finding. 5) If the application will initiate additional sessions without requiring authentication after logging out of the application, this is a CAT I finding. Web applications using autocomplete can be setup to store passwords and sensitive data. Many operating systems centrally control the autocomplete feature and it should be disabled. Workstations that do not have this feature disabled by default have the risk of storage of password information and sensitive information. Examples include public kiosks and home workstations connecting to the NIPRNet where this feature may be disabled. View the html pages that contain password and sensitive information to determine if autocomplete feature has been turned off.	Tested	Authentication Credentials are not stored or handled by the ECDR app.	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Example form html: <FORM AUTOCOMPLETE = "off"> Autocompletes are explained further at the Microsoft website. http://msdn.microsoft.com/en-us/library/ms533486(VS.85).aspx 6) If the application is configured to allow autocomplete for passwords, this is a CAT I finding. 7) If the application is configured to allow for sensitive information fields, this is a CAT II finding.						
IA-2	V-6156	Review source code (including global.asa, if present), configuration files, scripts, HTML file, and any ASCII files to locate any instances in which a password, certificate, or sensitive data is included in code. If credentials were found, check the file permissions on the offending file. 1) If the file permissions indicate that the file has no access control permissions (everyone can read or is world readable), this is a CAT I finding. 2) If there is a level of file protection that requires that at least authenticated users have read access, this is a CAT I finding. 3) If a level of protection exists that only administrators or those with a UID of 0 can read the file, this is a CAT II finding. The finding details should note specifically where the offending credentials or data were located and what resources they enabled.	Tested	Tested via HP Fortify. No hard coded passwords exist.	Pass	X		
IA-2 (1)	Identification and Authentication // Identification And Authentication (Organizational Users) | Network Access to Privileged Accounts		Tested		Pass		X	
IA-2 (1)		The information system implements multifactor authentication for network access to privileged accounts.	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-2 (11)	Identification and Authentication // Identification And Authentication (Organizational Users) | Remote Access - Separate Device		Tested		Pass		X	
IA-2 (11)		The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].	Tested		Pass		X	
IA-2 (12)	Identification and Authentication // Identification And Authentication (Organizational Users) | Acceptance of PIV Credentials		Tested		Pass		X	
IA-2 (12)		The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.	Tested		Pass		X	
IA-2 (2)	Identification and Authentication // Identification And Authentication (Organizational Users) | Network Access to Non-Privileged Accounts		Tested		Pass		X	
IA-2 (2)		The information system implements multifactor authentication for network access to non-privileged accounts.	Tested		Pass		X	
IA-2 (8)	Identification and Authentication // Identification And Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant		Tested		Pass		X	
IA-2 (8)		The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	Tested		Pass		X	
IA-2 (9)	Identification and Authentication // Identification And Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant		Tested		Pass		X	
IA-2 (9)		The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	Tested		Pass		X	
IA-5	Identification and Authentication // Authenticator Management		Tested		Pass		X	
IA-5		The organization manages information system authenticators by:	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-5	IA-5a.	Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;	Tested		Pass		X	
IA-5	IA-5b.	Establishing initial authenticator content for authenticators defined by the organization;	Tested		Pass		X	
IA-5	IA-5c.	Ensuring that authenticators have sufficient strength of mechanism for their intended use;	Tested		Pass		X	
IA-5	IA-5d.	Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;	Tested		Pass		X	
IA-5	IA-5e.	Changing default content of authenticators prior to information system installation;	Tested		Pass		X	
IA-5	IA-5f.	Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;	Tested		Pass		X	
IA-5	IA-5g.	Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];	Tested		Pass		X	
IA-5	IA-5h.	Protecting authenticator content from unauthorized disclosure and modification;	Tested		Pass		X	
IA-5	IA-5i.	Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and	Tested		Pass		X	
IA-5	IA-5j.	Changing authenticators for group/role accounts when membership to those accounts changes.	Tested		Pass		X	
IA-5 (1)	Identification and Authentication // Authenticator Management | Password-Based Authentication		Tested		Pass		X	
IA-5 (1)		The information system, for password-based authentication:	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-5 (1)	IA-5 (1)(a)	Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];	Tested		Pass		X	
IA-5 (1)	IA-5 (1)(b)	Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];	Tested		Pass		X	
IA-5 (1)	IA-5 (1)(c)	Stores and transmits only cryptographically-protected passwords;	Tested		Pass		X	
IA-5 (1)	IA-5 (1)(d)	Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];	Tested		Pass		X	
IA-5 (1)	IA-5 (1)(e)	Prohibits password reuse for [Assignment: organization-defined number] generations; and	Tested		Pass		X	
IA-5 (1)	IA-5 (1)(f)	Allows the use of a temporary password for system logons with an immediate change to a permanent password.	Tested		Pass		X	
IA-5 (11)	Identification and Authentication // Authenticator Management | Hardware Token-Based Authentication		Tested		Pass		X	
IA-5 (11)		The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].	Tested		Pass		X	
IA-5 (13)	Identification and Authentication // Authenticator Management | Expiration of Cached Authenticators		Tested		Pass		X	
IA-5 (13)		The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-5 (2)	Identification and Authentication // Authenticator Management | PKI-Based Authentication		Tested		Pass		X	
IA-5 (2)		The information system, for PKI-based authentication:	Tested		Pass		X	
IA-5 (2)	IA-5 (2)(a)	Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;	Tested		Pass		X	
IA-5 (2)	IA-5 (2)(b)	Enforces authorized access to the corresponding private key;	Tested		Pass		X	
IA-5 (2)	IA-5 (2)(c)	Maps the authenticated identity to the account of the individual or group; and	Tested		Pass		X	
IA-5 (2)	IA-5 (2)(d)	Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Tested		Pass		X	
IA-5 (2)	V-6127	This check is not applicable where application users are determined to have authorized access to the application and are not eligible to receive a CAC/DoD PKI certificate (e.g., retirees, dependents, etc.), as defined by DoDI 8520.2. 1) Ask the application representative if an application is PK-enabled. If the answer is no, this a finding. If the application is in a production environment, the application representative should be able to login to the application with a CAC. If the application resides on the SIPRNet, or in a test environment, the application representative may only have test certificates and should be able to login to the application with a soft certificate. Note: The certificates for this check do not need to be DoD approved certificates.	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If the application representative cannot log in to the application with either soft certificates or certificates from a CAC, it is a finding. Ask the application representative where the certificate store is for the application and verify there are the correct test or production certificates for user authentication. Make certain a certificate is required for user authentication. Ask the application representative to temporarily remove the certificate from the certificate store and authenticate to the application. For web application using Internet Explorer from the Tools Menu Select “Internet Options” Select “Content” tab Select “Certificates” Select “Remove” Other applications certificate stores will have similar features. 3) If the application representative can login to the application without either soft certificates or certificates stored on a CAC or another authentication mechanism, this is a CAT I finding for check APP3460. This finding should not be recorded for this check. 4) Ask the application representative to demonstrate encryption is being used for authentication. If the application representative cannot demonstrate encryption is being used, it is a finding.						
IA-5 (2)	V-6128	Policy: The designer and IAO will ensure PK-enabled applications are designed and implemented to use approved credentials authorized under the DoD PKI program. The IAO will ensure the PK-enabled applications are configured to honor only approved DoD PKI certificates. If the application is not PK-enabled, this check is not applicable. If the application resides on the SIPRNet and PKI infrastructure is unavailable, this check is not applicable. Ask whether the application utilizes PKI certificates other than DoD PKI and External Certification	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Authority (ECA) certificates. Verify the certificate used in authentication in APP3280. Internet Explorer can be used to view certificate information: Select “Tools” Select “Internet Options” Select “Content” tab Select “Certificates” Select the certificate used for authentication: Click “View” Select “Details” tab Select “Issuer” If the application utilizes PKI certificates other than DoD PKI and ECA certificates, this is a finding.						
IA-5 (2)	V-6129	If the application is not PK-enabled, this check is not applicable. If the application resides on the SIPRNet and PKI infrastructure is unavailable, this check is not applicable. This check is not applicable where system users are determined to be information privileged individuals, volunteers, or reservists, as required in the DoDI 8520.2. DoD test certificates can be obtained from the following website: http://jitc.fhu.disa.mil/pki/lab2.html Note: Before executing this check, the following certificate types need to be obtained: • Expired • Revoked • Improperly Signed If the application is PK-enabled and is not using DoD PKI certificates, the application representative will need to provide these certificates. If the application is a web-application that utilizes client certificates, validate the proper functioning	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		of the PKI-functionality using a laptop configured for the Application SRR using an expired and revoked certificate. This laptop contains three user profiles: One with a revoked certificate, one with an expired certificate, and one with an improperly signed certificate. Log on each of the user accounts for which there is an associated “bad certificate” profile and perform selected functions in the application that require the use of a certificate (e.g., authentication). 1) If the expired, revoked, or improperly signed certificate can be used for application functions, it is a finding. Also, review the web server’s configuration to ascertain whether appropriate certificate validity checks are occurring. 2) If the web server does not check for and deny expired, revoked, or improperly signed certificates, it is a finding. If the application is not a web-application, work with an application SA to identify PK-enabled application functions, and then sequentially install the invalid certificates, testing each of the functions against each of the certificates. 3) Any successful use of any of the invalid certificates is a finding. If a finding is found in any of the preceding steps, document the details of the finding to include the following: • Which of the invalid certificates was accepted (potentially more than one). • The specific application functions that accepted the invalid certificate. *Note: Do not use (WS-Security, SAML, and XML) security libraries that do not perform full certificate validation adequately. Checking should include the certificate against the CA’s Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP).						
IA-5 (2)	V-6168	Ask the application SA or developer if the application enables clients to authenticate to the server or the application it is communicating with. The most common example of this type of authentication is when a client validates a server’s PKI certificate when initiating an SSL or IPSEC connection.	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		1) If the SA or developer answers that this capability is not present, this is a finding. If the SA or developer states that the capability is present, validate this by logging on to each component that supports authentication of servers. For web applications, note cases in which the client browser issues a warning that the server's certificate is not valid. Reasons include: • A trusted certificate authority did not issue the certificate • The certificate has expired • The name of the certificate does not match the URL of the page you are trying to view The client application should provide a function to allow or disallow the server access to the client application. The server must be setup with a certificate for identification. Determine if the application checks for server authentication before allowing the user to continue. The server's certificate should be checked by the user's web browser or client application. 2) If there is no server certificate or the client application does not validate the server certificate, it is a finding.						
IA-5 (7)	Identification and Authentication // Authenticator Management | No Embedded Unencrypted Status Authenticators		Tested	Tested using HP Fortify	Pass	X		
IA-5 (7)		The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	Tested	Tested using HP Fortify	Pass	X		
IA-6	Identification and Authentication // Authenticator Feedback		Tested		Pass		X	
IA-6		The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Tested		Pass		X	
IA-7	Identification and Authentication // Cryptographic Module Authentication		Tested		Pass		X	
IA-7		The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
IA-8	Identification and Authentication // Identification And Authentication (Non-Organizational Users)		Tested		Pass		X	
IA-8		The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Tested		Pass		X	
IA-8 (1)	Identification and Authentication // Identification And Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies		Tested		Pass		X	
IA-8 (1)		The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	Tested		Pass		X	
IA-8 (2)	Identification and Authentication // Identification And Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials		Tested		Pass		X	
IA-8 (2)		The information system accepts only FICAM-approved third-party credentials.	Tested		Pass		X	
IA-8 (3)	Identification and Authentication // Identification And Authentication (Non-Organizational Users) | Use of FICAM-Approved Products		Tested		Pass		X	
IA-8 (3)		The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.	Tested		Pass		X	
IA-8 (4)	Identification and Authentication // Identification And Authentication (Non-Organizational Users) | Use of FICAM-Issued Products		Tested		Pass		X	
IA-8 (4)		The information system conforms to FICAM-issued profiles.	Tested		Pass		X	
PL-1	Planning // Security Planning Policy And Procedures		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1	PL-1a.	Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
PL-1	PL-1a.1.	A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1	PL-1a.2.	Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1	PL-1b.	Reviews and updates the current:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1	PL-1b.1.	Security planning policy [Assignment: organization-defined frequency]; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-1	PL-1b.2.	Security planning procedures [Assignment: organization-defined frequency].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-2	Planning // System Security Plan		Tested		Pass	X		
PL-2		The organization:	Tested		Pass	X		
PL-2	PL-2a.	Develops a security plan for the information system that:	Tested		Pass	X		
PL-2	PL-2a.1.	Is consistent with the organization's enterprise architecture;	Tested		Pass	X		
PL-2	PL-2a.2.	Explicitly defines the authorization boundary for the system;	Tested		Pass	X		
PL-2	PL-2a.3.	Describes the operational context of the information system in terms of missions and business processes;	Tested		Pass	X		
PL-2	PL-2a.4.	Provides the security categorization of the information system including supporting rationale;	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
PL-2	PL-2a.5.	Describes the operational environment for the information system and relationships with or connections to other information systems;	Tested		Pass	X		
PL-2	PL-2a.6.	Provides an overview of the security requirements for the system;	Tested		Pass	X		
PL-2	PL-2a.7.	Identifies any relevant overlays, if applicable;	Tested		Pass	X		
PL-2	PL-2a.8.	Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and	Tested		Pass	X		
PL-2	PL-2a.9.	Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;	Tested		Pass	X		
PL-2	PL-2b.	Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];	Tested		Pass	X		
PL-2	PL-2c.	Reviews the security plan for the information system [Assignment: organization-defined frequency];	Tested		Pass	X		
PL-2	PL-2d.	Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and	Tested		Pass	X		
PL-2	PL-2e.	Protects the security plan from unauthorized disclosure and modification.	Tested		Pass	X		
PL-2	Planning // System Security Plan		Tested		Pass	X		
PL-2	V-16775	Interview the application representative to determine if the system documentation has identified the Mission Assurance Category (MAC) and confidentiality levels of the application. 1) If no system documentation exists that identifies the MAC and confidentiality levels, it is a finding.	Tested	MAC and CL is not used for Software or RMF	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
PL-2	V-16786	Ask the application representative to review the installation guide to determine what functionality is installed and enabled by default on installation of the application. Examples may include the following: Functions that send information back to the vendor. E-mail functions enabled when not required for functionality. 1) If the application installs with functionality which is unnecessary and enabled by default, it is a finding.	Tested	The ECDR app is an relatively simple application that converts a REST query into a Java call. Only neccesary functionality is enabled. No configurations exist to enable/disable functionality.	Pass	X		
PL-2	V-16837	Interview the application representative and determine if all the application components are under maintenance. The entire application may be covered by a single maintenance agreement. The application should be decommissioned if maintenance or security support is no longer being provided by the vendor or by the development staff of a custom developed application. 1) If the application or any of the application components are not being maintained, it is a finding.	Tested	Sourecode is released under LGPL and is available to be maintained by anyone.	Sponsor			X
PL-2	V-16838	Interview the application representative to determine if provisions are in place to notify users when an application is decommissioned. 1) If provisions are not in place to notify users when an application is decommissioned, it is a finding.	Tested	Hosting Environment is outside the scope of this evaluation	NA			X
PL-2	V-6145	The IAO will ensure the classification guide for the application data exists and is available to users. If the application does not process classified information, this check is not applicable. The application may already be covered by a higher level program or other classification guide. If classification guide is not written specifically to the application, the sensitive application data should be reviewed to determine whether it is contained in the classification guide. DoD 5200.1-R, January 1997 identifies requirements for security classification and/or declassification guides (http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf). Security classification guides shall provide the following information:	Tested	Hosting Environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		• Identify specific items, elements, or categories of information to be protected. • State the specific classification to be assigned to each item or element of information and, when useful, specify items of information that are unclassified. • Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from automatic declassification. • State a concise reason for classification for each item, element, or category of information that, at a minimum, cites the applicable classification categories in Section 1.5 of E.O. 12958. • Identify any special handling caveats that apply to items, elements, or categories of information. • Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of that approval. • Provide a point-of-contact for questions about the guide and suggestions for improvement. • For information exempted from automatic declassification because its disclosure would reveal foreign government information or violate a statute, treaty, or international agreement, the security classification guide will identify the government or specify the applicable statute, treaty, or international agreement, as appropriate. 1) If the security classification guide does not exist, or does not contain data elements and their classification, it is a finding.						
PL-2	V-6151	Examine the configuration of the servers. Determine what software is installed on the servers. Determine which services are needed for the application by examining the application design and accreditation documentation and interviewing the application representative. For example, in cases where two web servers (IIS and Apache) are installed, and only one is being used. 1) If there are services or software present not needed for the application, it is a finding.	Tested	Hosting Environment is outside the scope of this evaluation	NA			X
PL-2	V-6197	The Program Manager will ensure all appointments to required IA roles are established in writing to include assigned duties and appointment criteria, such as training, security clearance, and IT designation. The IAO will ensure all appointments to required IA roles are established in writing to include assigned duties and appointment criteria such as training, security clearance, and IT designation. Interview the application representative and validate that the required IA roles are established in writing. These roles are DAA and the IAM/IAO. This written notification must include assigned duties and appointment criteria such as training, security clearance, and IT-designation.	Tested	Hosting Environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		If a traditional review is conducted at the same time as the application review, this check is not applicable. Also validate a SSP exists and describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response). 1) If the SSP does not exist or is incomplete, it is a finding. 2) If the IA Roles and assigned duties and appointment criteria are not made in writing, it is a finding. Ask site personnel which IAO or IAM for the systems/application is part of the application review. 3) If the IAO or IAM is unknown, or not assigned, this is a finding.						
PL-7	Planning // Security Concept of Operations		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-7		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-7	PL-7a.	Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-7	PL-7b.	Reviews and updates the CONOPS [Assignment: organization-defined frequency].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	Planning // Information Security Architecture		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
PL-8	PL-8a.	Develops an information security architecture for the information system that:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	PL-8a.1.	Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	PL-8a.2.	Describes how the information security architecture is integrated into and supports the enterprise architecture; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	PL-8a.3.	Describes any information security assumptions about, and dependencies on, external services;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	PL-8b.	Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PL-8	PL-8c.	Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
PM-6	Program Management // Information Security Measures of Performance		Tested		Pass	X		
PM-6		The organization develops, monitors, and reports on the results of information security measures of performance.	Tested		Pass	X		
RA-1	Risk Assessment // Risk Assessment Policy And Procedures		Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1		The organization:	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1	RA-1a.	Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1	RA-1a.1.	A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1	RA-1a.2.	Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
RA-1	RA-1b.	Reviews and updates the current:	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1	RA-1b.1.	Risk assessment policy [Assignment: organization-defined frequency]; and	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-1	RA-1b.2.	Risk assessment procedures [Assignment: organization-defined frequency].	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	Risk Assessment // Risk Assessment		Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3		The organization:	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	RA-3a.	Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	RA-3b.	Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	RA-3c.	Reviews risk assessment results [Assignment: organization-defined frequency];	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	RA-3d.	Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
RA-3	RA-3e.	Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	Tested	Using DoD RMF Risk Assesment Policy and Report	Pass	X		
SA-1	System and Services Acquisition // System And Services Acquisition Policy And Procedures		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-1		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1a.	Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1a.1.	A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1a.2.	Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1b.	Reviews and updates the current:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1b.1.	System and services acquisition policy [Assignment: organization-defined frequency]; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-1	SA-1b.2.	System and services acquisition procedures [Assignment: organization-defined frequency].	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-10		System and Services Acquisition // Developer Configuration Management	Tested		Pass	X		
SA-10		The organization requires the developer of the information system, system component, or information system service to:	Tested		Pass	X		
SA-10	SA-10a.	Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];	Tested		Pass	X		
SA-10	SA-10b.	Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];	Tested		Pass	X		
SA-10	SA-10c.	Implement only organization-approved changes to the system, component, or service;	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-10	SA-10d.	Document approved changes to the system, component, or service and the potential security impacts of such changes; and	Tested		Pass	X		
SA-10	SA-10e.	Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	Tested		Pass	X		
SA-10 (1)	System and Services Acquisition // Developer Configuration Management | Software/ Firmware Integrity Verification		Tested	Hosting platform would need to use a tool like Tripwire to monitor WebApp files. The Webapp cannot monitor itself.	Pass		X	
SA-10 (1)		The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	Tested	Hosting platform would need to use a tool like Tripwire to monitor WebApp files. The Webapp cannot monitor itself.	Pass		X	
SA-11	System and Services Acquisition // Developer Security Testing and Evaluation		Tested		Pass	X		
SA-11		The organization requires the developer of the information system, system component, or information system service to:	Tested		Pass	X		
SA-11	SA-11a.	Create and implement a security assessment plan;	Tested		Pass	X		
SA-11	SA-11b.	Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];	Tested		Pass	X		
SA-11	SA-11c.	Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;	Tested		Pass	X		
SA-11	SA-11d.	Implement a verifiable flaw remediation process; and	Tested		Pass	X		
SA-11	SA-11e.	Correct flaws identified during security testing/evaluation.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-11 (1)	System and Services Acquisition // Developer Security Testing and Evaluation | Static Code Analysis		Tested	Using HP Fortify and Coverity	Pass	X		
SA-11 (1)		The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Tested	Using HP Fortify and Coverity	Pass	X		
SA-11 (2)	System and Services Acquisition // Developer Security Testing and Evaluation | Threat and Vulnerability Analyses		Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-11 (2)		The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-11 (4)	System and Services Acquisition // Developer Security Testing and Evaluation | Manual Code Reviews		Tested	Conducted using Reviewable.io	Pass	X		
SA-11 (4)		The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].	Tested	Conducted using Reviewable.io	Pass	X		
SA-11 (5)	System and Services Acquisition // Developer Security Testing and Evaluation | Penetration Testing/ Analysis		Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-11 (5)		The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [Assignment: organization-defined breadth/depth] and with [Assignment: organization-defined constraints].	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-11 (6)	System and Services Acquisition // Developer Security Testing and Evaluation| Attack Surface Reviews		Tested		Pass	X		
SA-11 (6)		The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-11 (7)	System and Services Acquisition // Developer Security Testing and Evaluation | Verify Scope of Testing/ Evaluation		Tested		Pass	X		
SA-11 (7)		The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [Assignment: organization-defined depth of testing/evaluation].	Tested	SAT	Pass	X		
SA-12	System and Services Acquisition // Supply Chain Protection		Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-12		The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-12 (9)	System and Services Acquisition // Supply Chain Protection | Operations Security		Tested	No DD 254 was issued that required following an OPSEC plan	Pass	X		
SA-12 (9)		The organization employs [Assignment: organization-defined Operations Security (OPSEC) safeguards] in accordance with classification guides to protect supply chain-related information for the information system, system component, or information system service.	Tested	No DD 254 was issued that required following an OPSEC plan	Pass	X		
SA-15	System and Services Acquisition // Development Process, Standards, and Tools		Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15		The organization:	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-15	SA-15a.	Requires the developer of the information system, system component, or information system service to follow a documented development process that:	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15	SA-15a.1.	Explicitly addresses security requirements;	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15	SA-15a.2.	Identifies the standards and tools used in the development process;	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15	SA-15a.3.	Documents the specific tool options and tool configurations used in the development process; and	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15	SA-15a.4.	Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-15	SA-15b.	Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].	Tested	For the ECDR, the cost of developing a development plan would cost about as much as the total development. Therefore, with only a team of 3 the development team did not develop a development plan.	Failed			X
SA-15 (1)	System and Services Acquisition // Development Process, Standards, and Tools | Quality Metrics		Tested	Quality Metrics were not defined at the beginning of the development.	Failed			X
SA-15 (1)		The organization requires the developer of the information system, system component, or information system service to:	Tested	Quality Metrics were not defined at the beginning of the development.	Failed			X
SA-15 (1)	SA-15 (1)(a)	Define quality metrics at the beginning of the development process; and	Tested	Quality Metrics were not defined at the beginning of the development.	Failed			X
SA-15 (1)	SA-15 (1)(b)	Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].	Tested	Quality Metrics were not defined at the beginning of the development.	Failed			X
SA-15 (11)	System and Services Acquisition // Development Process, Standards, and Tools | Archive Information System/ Component		Tested		Pass	X		
SA-15 (11)		The organization requires the developer of the information system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security review.	Tested		Pass	X		
SA-15 (2)	System and Services Acquisition // Development Process, Standards, and Tools | Security Tracking Tools		Tested	JIRA is used to track work in ECDR.	Pass	X		
SA-15 (2)		The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.	Tested	JIRA is used to track work in ECDR.	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-15 (3)	System and Services Acquisition // Development Process, Standards, and Tools | Criticality Analysis		Tested	The ECDR was built to a Gov't produced specification, therefore a criticality analysis is not neccesary or useful.	NA			X
SA-15 (3)		The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle].	Tested	ECDR is built to a Gov't specification. A criticality analysis is not neccesary.	NA			X
SA-15 (4)	System and Services Acquisition // Development Process, Standards, and Tools | Threat Modeling/ Vulnerability Analysis		Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (4)		The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that:	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (4)	SA-15 (4)(a)	Uses [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (4)	SA-15 (4)(b)	Employs [Assignment: organization-defined tools and methods]; and	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (4)	SA-15 (4)(c)	Produces evidence that meets [Assignment: organization-defined acceptance criteria].	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (5)	System and Services Acquisition // Development Process, Standards, and Tools | Attack Surface Resolution		Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-15 (5)		The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Tested		Pass	X		
SA-15 (6)	System and Services Acquisition // Development Process, Standards, and Tools | Continuous Improvement		Tested	The development team has not implemented an explicit process to continuously improve the development process.	Failed			X
SA-15 (6)		The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.	Tested	The development team has not implemented an explicit process to continuously improve the development process.	Failed			X
SA-15 (7)	System and Services Acquisition // Development Process, Standards, and Tools | Automated Vulnerability Analysis		Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (7)		The organization requires the developer of the information system, system component, or information system service to:	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (7)	SA-15 (7)(a)	Perform an automated vulnerability analysis using [Assignment: organization-defined tools];	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (7)	SA-15 (7)(b)	Determine the exploitation potential for discovered vulnerabilities;	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (7)	SA-15 (7)(c)	Determine potential risk mitigations for delivered vulnerabilities; and	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-15 (7)	SA-15 (7)(d)	Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].	Tested	Static Analysis, Threat Modeling, Fuzz Testing, Penetration Testing, and Third Party Vulnerability Analysis	Pass	X		
SA-15 (8)	System and Services Acquisition // Development Process, Standards, and Tools | Reuse of Threat/ Vulnerability Information		Tested	Threat Model compared to DDF Spatial	Pass	X		
SA-15 (8)		The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.	Tested	Threat Model compared to DDF Spatial	Pass	X		
SA-16	System and Services Acquisition // Developer-Provided Training		Tested	ECDR Does not contain any security relevant software.	NA			X
SA-16		The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17	System and Services Acquisition // Developer Security Architecture and Design		Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17		The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17	SA-17a.	Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17	SA-17b.	Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17	SA-17c.	Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (1)	System and Services Acquisition // Developer Security Architecture and Design | Formal Policy Model		Tested	ECDR Does not contain any security relevant software.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-17 (1)		The organization requires the developer of the information system, system component, or information system service to:	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (1)	SA-17 (1)(a)	Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security policy] to be enforced; and	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (1)	SA-17 (1)(b)	Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (2)	System and Services Acquisition // Developer Security Architecture and Design | Security- Relevant Components		Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (2)		The organization requires the developer of the information system, system component, or information system service to:	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (2)	SA-17 (2)(a)	Define security-relevant hardware, software, and firmware; and	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (2)	SA-17 (2)(b)	Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (3)	System and Services Acquisition // Developer Security Architecture and Design | Formal Correspondence		Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (3)		The organization requires the developer of the information system, system component, or information system service to:	Tested	The ECDR Contains no security relevant software	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-17 (3)	SA-17 (3)(a)	Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (3)	SA-17 (3)(b)	Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (3)	SA-17 (3)(c)	Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (3)	SA-17 (3)(d)	Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (3)	SA-17 (3)(e)	Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)	System and Services Acquisition // Developer Security Architecture and Design | Informal Correspondence		Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)		The organization requires the developer of the information system, system component, or information system service to:	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)	SA-17 (4)(a)	Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;	Tested	The ECDR Contains no security relevant software	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-17 (4)	SA-17 (4)(b)	Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)	SA-17 (4)(c)	Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)	SA-17 (4)(d)	Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (4)	SA-17 (4)(e)	Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.	Tested	The ECDR Contains no security relevant software	NA			X
SA-17 (5)	System and Services Acquisition // Developer Security Architecture and Design | Conceptually Simple Design		Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (5)		The organization requires the developer of the information system, system component, or information system service to:	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (5)	SA-17 (5)(a)	Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (5)	SA-17 (5)(b)	Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.	Tested	ECDR Does not contain any security relevant software.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-17 (6)	System and Services Acquisition // Developer Security Architecture and Design | Structure for Testing		Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (6)		The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate testing.	Tested	ECDR Does not contain any security relevant software.	NA			X
SA-17 (7)	System and Services Acquisition // Developer Security Architecture and Design | Structure for Least Privilege		Tested	Uses DDF Priveleges	Pass		X	
SA-17 (7)		The organization requires the developer of the information system, system component, or information system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.	Tested		Pass		X	
SA-2	System and Services Acquisition // Allocation Of Resources		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-2		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-2	SA-2a.	Determines information security requirements for the information system or information system service in mission/business process planning;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-2	SA-2b.	Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-2	SA-2c.	Establishes a discrete line item for information security in organizational programming and budgeting documentation.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-22	System and Services Acquisition // Unsupported System Components		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-22		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-22	SA-22a.	Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-22	SA-22b.	Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-3	System and Services Acquisition // System Development Life Cycle		Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-3		The organization:	Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-3	SA-3a.	Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;	Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-3	SA-3b.	Defines and documents information security roles and responsibilities throughout the system development life cycle;	Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-3	SA-3c.	Identifies individuals having information security roles and responsibilities; and	Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-3	SA-3d.	Integrates the organizational information security risk management process into system development life cycle activities.	Tested	3 collaborative team member use Agile methodology. One member is the security engineer that monitors and manages risk.	Pass	X		
SA-4	System and Services Acquisition // Acquisition Process		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4		The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4a.	Security functional requirements;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4b.	Security strength requirements;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4c.	Security assurance requirements;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4d.	Security-related documentation requirements;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4e.	Requirements for protecting security-related documentation;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4f.	Description of the information system development environment and environment in which the system is intended to operate; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4	SA-4g.	Acceptance criteria.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SA-4 (1)	System and Services Acquisition // Acquisition Process | Functional Properties of Security Controls		Tested	No Native security features	Pass	X		
SA-4 (1)		The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Tested	No Native Security Features	Pass	X		
SA-4 (10)	System and Services Acquisition // Acquisition Process | Use of Approved PIV Products		Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (10)		The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	Tested		Pass		X	
SA-4 (2)	System and Services Acquisition // Acquisition Process | Design/ Implementation Information for Security Controls		Tested	No Native Security Features	Pass	X		
SA-4 (2)		The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].	Tested	No Native Security Features	Pass	X		
SA-4 (3)	System and Services Acquisition // Acquisition Process | Development Methods/ Techniques/ Practices		Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SA-4 (3)		The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes].	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SA-4 (3)	V-16776	The Program Manager will ensure the development team follows a set of coding standards. The Program Manager will ensure the development team creates a list of unsafe functions to avoid and document this list in the coding standards. The Designer will follow the established coding standards established for the project. The Designer will not use unsafe functions documented in the project coding standards. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Interview the application representative to determine if a documented set of coding standards exists. Ask the application representative to demonstrate coding standards are being followed by reviewing a sample of code. Also, check the coding standards for a list of unsafe functions or section documenting there are no unsafe functions. 1) If no coding standards exist at an organizational or project level, it is a finding. 2) If documented coding standards are not being followed, it is a finding. 3) If there is no documented list of unsafe functions, or the coding standards do not document that there are no unsafe functions (for that particular language), it is a finding.						
SA-4 (3)	V-16787	Ask the application representative for code review results from the entire application or the documented code review process. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. If the results are provided from a manual code review, the application representative will need to demonstrate how secure design principle vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify secure design principle vulnerabilities, this is a CAT I finding. 2) If code analysis tools are used to perform a code review and errors have not been fixed, this is a CAT II finding.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-16804	Verify the application does not grant access solely based on a resource name (e.g., username, IP address, machine name). Also, verify a username with a blank password does not grant access to the application. 1) If authentication is granted based on a resource name only, it is a finding.	Tested	Authentication is managed by the Hosting systems DIB Integration	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-16806	Ask the application representative to review web pages, and determine if the application sets the character set. Perl After the last header look for print "Content-Type: text/html; charset=utf-8\n\n"; PHP. Look for the header() function before any content is generated header('Content-type: text/html; charset=utf-8'); Java Servlets. Look for the setContentType method on the ServletResponse object Objectname.setContentType ("text/html;charset=utf-8"); JSP. Look for a page directives <%@ page contentType="text/html; charset=UTF-8" %> ASP Look for Response.charset <%Response.charset="utf-8"%> ASP.Net Look for Response.ContentEncoding Response.ContentEncoding = Encoding.UTF8; 1) If the application representative cannot demonstrate the above, it is a finding.	Tested		Pass			
SA-4 (3)	V-16807	SQL Injections attacks can be used to bypass the login to the application or to provide authenticated user access to data that should not normally be provided by the application. Test applications using Oracle, Microsoft SQL Server, and other backend databases by putting a single ' in any of the fields used to login. Submit the form and check for a server error 400. If the error occurs, the application is not properly validating input fields. If an invalid user or password	Tested	Authentication is managed by the Hosting systems DIB Integration	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		message is returned upon submitting the web form, the application is at least minimally protected. Fill in login fields with potentially valid user names (e.g., admin, system, root, administrator) with a comment field to ignore the rest of the SQL query. Fill in the password fields with any values and submit the form. username' -- username' # username'/* 1) If the application bypasses user authentication with these inputs, this is a CAT I finding. Try to append the "or" operator with a true value "1=1" and comment field. This will test if a SQL query could be passed into the application for execution. Fill in the login and password fields one at a time with the inputs below and submit the form. ' or 1=1-- ' or 1=1# ' or 1=1/* ') or 1=1-- ') or 1=1# ') or 1=1/* 2) If the application bypasses user authentication with these inputs, this is a CAT I finding. Also other fields not associated with the login fields should be tested. Fill in the each of the inputs one at a time with the inputs below, and submit the form. ' or 1=1-- ' or 1=1# ' or 1=1/* ') or 1=1-- ') or 1=1#						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		') or 1=1/* 3) If the application provides an authenticated user access or elevated access to the application to data, this is a CAT I finding. Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the application representative cannot provide results from a code review, then ask the application representative to demonstrate how the application meets the requirements below. Identify from the code review results or the application representative demonstration how the application: - Uses prepared statements for SQL queries - Does not provide direct access to tables (e.g. access is provided by views and stored procedures) - Does not use concatenation or use replacement to build SQL queries 4) If the results are not provided from a manual code review or automated tool or the application representative cannot demonstrate the application uses prepared statements for SQL queries, this is a CAT II finding. 5) If the results are not provided from a manual code review or automated vulnerability scanning tool, or the application representative cannot demonstrate the application does not use concatenation or use replacement to build SQL queries, this is a CAT II finding. 6) If the results are not provided from a manual code review or automated vulnerability scanning tool, or the application representative cannot demonstrate the application does not directly accesses tables in a database, this is a CAT II finding. 7) If APP3500 is a finding due to the application account being a member of the Administrators group (Windows), has a UID of 0 (i.e., is equivalent to root in UNIX), is a member of the SYSAdmin fixed server role in SQL Server, or has DDL privileges, the finding should be upgraded to a CAT I.						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		*Note Web services are subject to the same coding practices of other web application code (e.g., SQL Injection).						
SA-4 (3)	V-16808	Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool or use static analysis tools that are known to find this class of vulnerability with few false positives. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how integer overflow vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify integer overflow vulnerabilities, it is a finding. Examples of integer overflow vulnerabilities can be obtained from the OWASP website.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-16809	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how format string vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify format string vulnerabilities, it is a finding. Examples of format string vulnerabilities can be obtained from the OWASP website.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-16810	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how command injection vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		code reviews are performed to identify command injection vulnerabilities, it is a finding. Examples of Command Injection vulnerabilities can be obtained from the OWASP website. *Note: Web services are subject to the same coding practices of other web application code (e.g., command injection).						
SA-4 (3)	V-16811	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how XSS vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify cross site scripting vulnerabilities, this is a CAT I finding. Perform query string manipulation testing to determine if the user bypasses access control functions to gain data that should be restricted based on the user's security level or role. For example, if a query string, such as www.testweb.mil/apppage.asp?xyz=113&asd=185, gives the user access to data for data identifier number 185. Try to resubmit the query string with another three digit number (e.g., 186) to see if that data is displayed. If this data can be displayed through reports or other access points in the application, this would not be considered a finding. 2) If data displayed in the query manipulation testing is above the user's security level or role, this is a CAT II finding. For script tag embedding, select a text field of the application that accepts at least 15 characters. Try to input a script tag (script) into the field. If the data is accepted without an error, access the data entered via the application (this process will vary depending upon the application). 3) If the script tag in its entirety is displayed within the application, this is a CAT II finding. Mitigate XSS vulnerabilities by using HTTP-only cookies. Examine any cookies used while the application is being executed. Verify the HttpOnly flag has been set for all cookies.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		4) If the HttpOnly flag has not been set for all cookies, this is a CAT II finding. HttpOnly cookies are explained further at the Microsoft website: http://msdn.microsoft.com/en-us/library/ms533046.aspx Examples of XSS vulnerabilities can be obtained from the OWASP website.						
SA-4 (3)	V-16812	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how canonical representation vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify canonical representation vulnerabilities this is a finding. Examples of Canonical Representation vulnerabilities can be obtained from the OWASP website.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-16813	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details. If the results are provided from a manual code review, the application representative will need to demonstrate how hidden field vulnerabilities are identified during code reviews. Hidden fields or input parameters that utilize randomly generated token values used to address Cross Site Request Forgery (CSRF) attacks and are not used for access control are not applicable. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify hidden field vulnerabilities, this is a CAT I finding. 2) If the code review results are provided and hidden field vulnerabilities exist for user authentication, this is a CAT I finding.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		3) If the code review results are provided and hidden field vulnerabilities exist allowing users to access unauthorized information, this is a CAT II finding.						
SA-4 (3)	V-16815	Policy: The designer will ensure the application is not vulnerable to race conditions. The designer will ensure the application does not use global variables when local variables could be used. The designer will ensure a multi-threaded application uses thread safe functions when threads are accessing the same object or data. The Designer will ensure global resources are locked before being accessed by the application. Check: If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool. The review results should include all web services used in the application. If the results are provided from a manual code review, the application representative will need to demonstrate how the following vulnerabilities are identified during code reviews: • Race conditions • Using global variables when local variables could be used • Multi-threaded application uses thread safe functions • Global resources are locked before being accessed by the application 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify these vulnerabilities, it is a finding.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Examples of race conditions vulnerabilities can be obtained from the OWASP website.						
SA-4 (3)	V-16824	Ask the application representative if an individual has been designated to test for security flaws. 1) If no individual has been designated to test for security flaws, it is a finding.	Tested	Bobby King	Pass	X		
SA-4 (3)	V-16828	Ask the application representative to provide code coverage statistics maintained for the application. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If these code coverage statistics do not exist, it is a finding.	Tested	https://coveralls.io/r/di2e/ecdr	Pass	X		
SA-4 (3)	V-16829	Ask the application representative to provide evidence of automated code reviews. This will be in the form of a test plan or methodology which identifies application architecture and components as well as a formal report provided by the automated code review tool plus manual testing results. This requirement requires access to the application source code, if the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If an automated application code review is not performed, this is a finding. 2) If analysis of code review results is not performed, this is a finding. 3) If all application code is not being reviewed, this is a finding. 4) If the code review report includes coding errors that have not been fixed, this is a finding. If identified coding errors have been fixed, this is not a finding. 5) If the code reviews indicate the existence of hard-coded IPv4 or IPV6 addresses, it is a finding.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-16830	Ask the application representative to demonstrate that the configuration management repository captures flaws in the code review process. The configuration management repository may consist of a separate application for capturing code defects. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If there is no configuration management repository or the code review flaws are not captured in the configuration management repository, it is a finding.	Tested	https://github.com/di2e/ecdr https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SA-4 (3)	V-16831	Ask the application representative to provide vulnerability test procedures and vulnerability test results. Ask the application representative to provide the settings that were used to conduct the vulnerability testing. Verify the automated vulnerability scanning tool was appropriately configured to assure as complete a test as possible of the application architecture components. E.g. if the application includes a web server, web server tests must be included. 1) If the application test procedures and test results do not include active vulnerability and fuzz testing this is a finding. 2) If the vulnerability scan results include critical vulnerabilities, this is a finding. 3) If the vulnerability scanning tests are not relevant to the architecture of the application, it is a finding. 4) If the vulnerability scan report includes informational and/or non-critical results this is not a finding. 5) If previously identified vulnerabilities have subsequently been resolved, this is not a finding.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-16832	Ask the application representative to demonstrate how security flaws are integrated into the project plan. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If security flaws are not addressed in the project plan or there is no process to introduce security flaws into the project plan, it is a finding.	Tested	https://github.com/di2e/ecdr https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SA-4 (3)	V-16833	Ask the application representative to review the servers where the application is deployed. Also, ask what other applications are deployed on those servers. 1) If a mission critical (MAC I) application is deployed on the same server as other applications, it is a finding.	Tested	The deployed environment is out of scope of this review.	NA			X
SA-4 (3)	V-16839	Ask the application representative to review the threat model for DoS attacks. Verify the mitigation for DoS attacks are implemented from the threat model. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If the mitigation from the threat model for DoS attacks are not implemented, it is a finding.	Tested		Pass	X		
SA-4 (3)	V-19689	Ask the application representative for design documentation, review the design documentation and ensure the application employs methods for XML schema validation and disables use of inline XML Document Type Definition (DTD) schemas in XML parsing objects. Managing DTD parsing behavior is a key to preventing the invocation of XML bombs. DTD parsing is controlled within the .Net application framework in .NET applications. 1) If the design document does not exist or address the specified web service, it is a finding. 2) If the Application does not employ any method of schema validation, it is a finding.	Tested	ECDR Does not use XML	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		3) If the Application does not disable the use of inline XML Document Type Definition (DTD) schemas it is a finding.						
SA-4 (3)	V-19690	Ask the application representative for the design document. Review the design document for web services. Review the design and verify there is redundancy for web services. Redundancy may be accomplished by deploying the same web service over multiple network devices. For MAC I systems: 1) If the design document does not exist or does not indicate the existence of redundant web services or the application representative is not able to demonstrate redundant web services, it is a finding. 2) For MAC II and MAC III systems if the design document does not exist, it is a finding. The requirement for redundant web services is NA for MAC II and MAC III	Tested	The deployed environment is out of scope of this review.	NA			X
SA-4 (3)	V-19691	Ask the application representative for the design document. Review the design document for web services. Review the design and verify web services have been implemented differently to prevent similar attacks from a complete DoS. For MAC I and MAC II systems: 1) If the design document does not exist or does not indicate web services have been implemented with different algorithms, this is a finding. For MAC III systems: 2) If the design document does not exist this is a finding.	Tested	STIG Check is untestable	NA			X
SA-4 (3)	V-19692	Ask the application representative for the design document. Review the design document for web services. Review the design and verify all web services can prioritize requests. Techniques used to prioritize web services include but are not limited to using Quality of Service (QoS) or some other means of reliable messaging such as WS_Reliability or WS_ReliableMessaging 1) For MAC I and MAC II systems; If the design document does not exist or does not indicate all web services can prioritize requests, this is a finding. 2) If the system is a MAC III system this requirement is NA	Tested	Messaging is not handled by the ECDR App	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-19693	Ask the application representative for execution flow diagrams. Review the execution flow diagrams and determine if all web services are covered in the flow diagrams. 1) If execution flow diagrams do not exist or are not complete, this is a finding.	Tested	In J2EE Web Apps Deadlock is caused when an application attempts to manage multiple threads. This is a bad practice that HP Fortify checks for, no issues were found for this.	Pass	X		
SA-4 (3)	V-19694	Ask the application representative to verify whether XML based web services are used within the application. If no XML based web services are used in the application, this check is not applicable. If XML based web services are used within the application, ask the application representative for a network diagram identifying the XML firewall placement. Review the network diagrams and determine if all web services are protected by the XML firewall. 1) If network diagrams do not exist or all web services are not protected by the XML firewall, it is a finding.	Tested	ECDR Uses only REST and JAVA Calls	NA			X
SA-4 (3)	V-19695	Ask the application representative for the design document. Review the design document for all web services. Review the design and verify all web services are able to detect resubmitted SOAP message requests. Look for the use of WS_Reliability or WS_ReliableMessaging standards. WS_Reliability or WS_ReliableMessaging syntax includes the use of "At-Most" semantics which guarantees that a duplicate message will not be delivered or "Exactly-Once" which guarantees a message will be delivered without duplication. If the application developer uses other reliable messaging standards to detect re-submitted messages, the developer should provide information as to how those standards meet this requirement. 1) If the design document does not indicate all web services are able to detect resubmitted SOAP message requests, this is a finding.	Tested	ECDR Does not use SOAP or SAML.	NA			X
SA-4 (3)	V-19696	If the application does not utilize UDDI registries or if the application utilizes the DISA PEO-GES managed UDDI registry and the DISA PEO-GES registry employs processes/procedures that control user access for publishing to the UDDI registry, this check is not applicable.	Tested	ECDR Does not use UDDI	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Ask the application representative for the URL for the WSDL for all web services used in the application. Download each WSDL entry using a web browser and verify each entry has been signed by a publisher certificate. 1) If all WSDL entries have not been signed, it is a finding.						
SA-4 (3)	V-19697	If the application does not utilize UDDI registries, this check is not applicable. Ask the application representative for design document and verify the version of the UDDI registry used. UDDI Version 3.0 and above repositories supports digital signatures for web services. 1) If the UDDI registry is not Version 3 or above, this is a finding.	Tested	ECDR Does not use UDDI	NA			X
SA-4 (3)	V-19698	If the application does not utilize UDDI registries, this check is not applicable. Ask the application representative to demonstrate UDDI publishing is restricted to authenticated users. 1) If application representative is unable to demonstrate UDDI publishing is restricted to authenticated users, it is a finding.	Tested	ECDR Does not use UDDI	NA			X
SA-4 (3)	V-19706	Verify the application environment is compliant with all DoD IPv6 Standards Profile for IPv6 Capable Products guidance for servers. 1) If the application environment is not compliant with all DoD IPv6 Standards Profile for IPv6 Capable Products guidance for servers, this is a finding.	Tested	Network Communication is not managed by the ECDR Web App	NA			X
SA-4 (3)	V-19707	Ask the application representative for the design document. Review the design document for application services supporting IPv6. Verify supporting application layer services (such as, File Transfer Protocol (FTP), Network File system (NFS), Hyper Text Transfer Protocol (HTTP)) have been upgraded and tested for IPv6. 1) If the supporting application layer services have not been upgraded and tested for IPv6, it is a finding.	Tested	Network Communication is not managed by the ECDR Web App	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Verify security functions have been updated for IPv6 addressing and network services. 2) If security functions have not been updated for IPv6 addressing and network services, it is a finding. Verify all software update, security update, driver updating, and automatic patching services which retrieve updates over a network connection have been updated to run over IPv6 transport. 3) If all software update, security update, driver updating, and automatic patching have not been updated to run over IPv6 transport, it is a finding. Verify all client-facing server interfaces have been upgraded for IPv6. 4) If all client-facing server interfaces have not been upgraded for IPv6, it is a finding.						
SA-4 (3)	V-19708	Ask the application representative for the design document. Review the design document for application services supporting IPv6. Verify configuration options for the application for IPv6 addresses. 1) If the application has not been upgraded to support IPv6 addresses, it is a finding. Verify configuration options for the application for IPv6 multicasting. 2) If the application has not been upgraded to support IPv6 multicasting, it is a finding.	Tested	Network Communication is not managed by the ECDR Web App	NA			X
SA-4 (3)	V-19709	Ask the application representative for the design document. Review the design document for application services supporting IPv6. Verify user interfaces, graphic user interface (GUI), and system management interfaces have been updated to support IPv6 addressing and functions. 1) If the application interfaces have not been upgraded to support IPv6 addressing and functions, it is a finding.	Tested	Network Communication is not managed by the ECDR Web App	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-21498	Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool. If the results are provided from a manual code review, the application representative will need to demonstrate how XML injection vulnerabilities are identified during code reviews. Using XML Schema Definition (XSD) Restrictions and XML Schema Regular Expressions can minimize XML injection attacks. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify XML injection vulnerabilities, it is a finding. Examples of XML Injection vulnerabilities can be obtained from the OWASP website.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-21500	Ask the application representative for code review results from the entire application. This can be provided as results from an automated code review tool. If the results are provided from a manual code review, the application representative will need to demonstrate how CSRF vulnerabilities are identified during code reviews. 1) If the results are not provided or the application representative cannot demonstrate how manual code reviews are performed to identify CSRF, it is a finding.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-21519	Ask the application representative for the design document. Review the design document for all software components. Ask the application representative for proof that the application and all of its components are supported. Examples of proof may include: design documentation that includes support information, support specific contract documentation, successful creation of vendor support tickets, web site toll free support phone numbers etcetera." If any of the software components are not supported by a vendor, it is a finding.	Tested	ECDR uses potentially unsupported open source software.	Failed			X
SA-4 (3)	V-22028	Examine the contents of a SOAP message using the SubjectConfirmation element. All messages should contain the NotOnOrAfter element. This can be accomplished with a protocol analyzer like Wireshark. 1) If SOAP messages do not contain NotOnOrAfter elements, it is a finding	Tested	ECDR Does not use SOAP or SAML.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-4 (3)	V-22029	Examine the contents of a SOAP message using the <Conditions> element, all messages should contain the NotBefore and NotOnOrAfter or OneTimeUse element when in a SAML Assertion. This can be accomplished using a protocol analyzer such as WireShark 1) If SOAP using the <Conditions> element do not contain NotBefore and NotOnOrAfter or OneTimeUse elements, it is a finding.	Tested	ECDR Does not use SOAP or SAML.	NA			X
SA-4 (3)	V-22030	Ask the application representative for the Design Document. Verify in the Design Document asserting parties for SAML assertions use FIPS approved random numbers in the generation of SessionIndex in the Element AuthnStatement. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If FIPS approved random numbers are not used in the generation of SessionIndex (in the Element AuthnStatement), it is a finding.	Tested	ECDR does not generate random numbers	NA			X
SA-4 (3)	V-22032	Examine the contents of a SOAP message using the OneTimeUse element, all messages should contain only one instance of a OneTimeUse element in a SAML assertion. This can be accomplished using a protocol analyzer such as WireShark 1) If SOAP message uses more than one, OneTimeUse element in a SAML assertion, it is a finding.	Tested	ECDR Does not use SOAP or SAML.	NA			X
SA-4 (3)	V-6148	Review the threat model and identify the following sections are present: • Identified threats • Potential mitigations • Mitigations selected based on risk analysis Detailed information on threat modeling can be found at the Open Web Application Security Project (OWASP) website. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable.	Tested	SAT	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		1) If the threat model does not exist, or does not have identified threats, potential mitigations, and mitigations selected based on risk analysis, as sections within the Threat Model, it is a finding. 2) If the threat model has not been updated to reflect the application release being reviewed, this is a finding. Verify the mitigations selected in the threat model have been implemented. 3) If the mitigations selected based on risk analysis have not been implemented, this is a finding. Review the identified threats from the each of the application's networked components. For example, a backend server may accept SQL queries and SSH connections and also have an NFS share. Next, examine firewall rules and router ACLs that prevent clients from reaching these access points, effectively reducing the area of the threat surface. For example, if the backend database accepts queries but is in an enclave where there are no user workstations and firewall rules allow only web traffic, this is not a finding. For each of the remaining access points, attempt to access these resources in a similar manner as the application would without utilizing the user interface (e.g., send SQL query using a tool outside of the application or attempt to access a share using command line utilities). 4) If a user can authenticate to any of these remaining access points outside of the intended user interface, this is a finding. The finding details should note the application component accessed and the method or tool used to access it.						
SA-4 (3)	V-6149	Ask the application representative if there is a documented process to remove code when it is no longer executed. Also ask if there is a documented process to ensure unnecessary code is not included into a release. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable.	Tested	Deadcoce check by HP Fortify	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The process may include the following: · Source code analysis tools · Development environments that indicate unused source code · Compiler options that detect unreachable code For a web-based application, conduct a spot check of the code directory (e.g., .html, .asp, .jsp, and .php files), sampling at least four files, and ensure the code is executed for the application. If a documented process is not in place, check at least 10 pieces of code. Search for possible 'include files' and scripts. Determine if the 'include files' and scripts exist. Examples of 'include files' and scripts: jsp <%@ include file="include.jsp" %> php <?php include("include.php"); ?> asp <!--#include file="include.html"--> js <script src="include.js" type="text/javascript"></script> 1) If 'include files' and scripts do not exist, it is a finding. 2) If other code is found that is not being used, this is a finding. Document the name of the file containing the offending code in the finding details. For Visual Basic or C/C++ and other applications verify that a documented process is in place to prevent unused source code from being introduced into the application. Verify the process by source code analysis tools results, development environment tools, compiler options or the mechanism documented by process that enforces unused source from being introduced into the application.						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		3) If the application representative does not have a documented policy or there is no evidence that mechanisms are in place to prevent the introduction of unused code into the application, this is a finding.						
SA-4 (3)	V-6155	Log on to the application and then attempt to log out. If this option is not available, ask the application representative to explain how this function is performed. 1) If the ability to log out is absent or is hidden to the extent most users cannot reasonably expect to easily find it, it is a finding.	Tested	Authentication is not handled by ECDR	NA			X
SA-4 (3)	V-6157	Search the source code for common URL prefixes and suffixes and to the extent feasible with available tools, NFS shares, NetBIOS shares and IP addresses. All such resources should be captured from configuration files (i.e., “http://”, ftp://, “.mil”, “.com”). 1) If any references are invalid, it is a finding.	Tested	1,258 Matches within the source code. All matches were either references to a namespace, a license reference, or a localhost URL.	Pass	X		
SA-4 (3)	V-6164	Ask the application representative for the test plans for the application. Examine the test plan to determine if testing was performed for invalid input. Invalid input includes presence of scripting tags within text fields, query string manipulation, and invalid data types and sizes. If the test plans indicate these types of tests were performed, only a small sampling of testing is required. If the test plans do not exist or do not indicate that these types of tests were performed, more detailed testing is required. Testing should include logging on to the application and entering invalid data. If there are various user types defined within the system, this test should be repeated for all user types. Test the application for invalid sizes and types. Test input fields on all pages/screens of the application. Try to exceed buffer limits on the input fields. Try to put wrong types of data in the input fields. For example, put character data in a numeric field. 1) If an unauthenticated user can enter invalid input to bypass access control mechanisms, this is a CAT I finding. 2) If an authenticated user can enter invalid input to gain elevated access, this is a CAT I finding. 3) If the application requires the entry of IP addresses is not capable of handling IPv6 formats that are 128 bits long, this is a CAT II finding.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		4) If the application is not capable of handling IPv6 formats and accepts characters that are of hexadecimal notation including colons, this is a CAT II finding.						
SA-4 (3)	V-6165	Ask the application representative for code review or scan results from the entire application. This can be provided as results from an automated code review or a vulnerability scanning tool. See section 5.4 of the Application Security and Development STIG for additional details on code review and tools. If the results are provided from a manual code review, the results will need to describe how buffer overflow vulnerabilities and functions vulnerable to buffer overflows are identified during code reviews. 1) If scan results are provided and buffer overflow vulnerabilities have been identified in the report, this is a finding. 2) If scan results are provided but do not include the scan configuration settings which show that the application was tested for buffer overflows, this is a finding. 3) If manual test results are provided and the report does not confirm the lack of buffer overflows and also describe how buffer overflows and functions vulnerable to buffer overflows are identified during the code review, this is a finding. *Note: For IPV6 capable applications, check existing libraries to ensure they are capable of processing the increased size of IPv6 addresses to avoid buffer overflows.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		
SA-4 (3)	V-6166	Use the error messages generated from APP3510 as input into this check. Ensure that the application provides error handling processes. The application code should not rely on internal system generated error handling. 1) If the errors are not being handled by the application, and are being processed by the underlying internal system, this is a CAT III finding. Inspect the verbiage of the message. Ensure that the application does not provide information that can be used by an attacker.	Tested	HP Fortify, Coverity, Reviewable.IO	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If any of the following types of errors are displayed, this is a CAT II finding. Error messages should not include variable names, variable types, SQL strings, or source code. Errors that contain field names from the screen and a description of what should be in the field should not be considered a finding.						
SA-4 (5)	System and Services Acquisition // Acquisition Process | System/ Component/ Service Configurations		Tested	No security configurations exist for ECDR	Pass	X		
SA-4 (5)		The organization requires the developer of the information system, system component, or information system service to:	Tested	No security configurations exist for ECDR	Pass	X		
SA-4 (5)	SA-4 (5)(a)	Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and	Tested	No security configurations exist for ECDR	Pass	X		
SA-4 (5)	SA-4 (5)(b)	Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	Tested	No security configurations exist for ECDR	Pass	X		
SA-4 (9)	System and Services Acquisition // Acquisition Process | Functions/ Ports/ Protocols/ Services in Use		Tested	https://confluence.di2e.net/display/ECDR/Ports%2C+Protocols%2C+and+Services	Pass	X		
SA-4 (9)		The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	Tested	https://confluence.di2e.net/display/ECDR/Ports%2C+Protocols%2C+and+Services	Pass	X		
SA-5	System and Services Acquisition // Information System Documentation		Tested		Pass	X		
SA-5		The organization:	Tested		Pass	X		
SA-5	SA-5a.	Obtains administrator documentation for the information system, system component, or information system service that describes:	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-5	SA-5a.1.	Secure configuration, installation, and operation of the system, component, or service;	Tested		Pass	X		
SA-5	SA-5a.2.	Effective use and maintenance of security functions/mechanisms; and	Tested		Pass	X		
SA-5	SA-5a.3.	Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;	Tested		Pass	X		
SA-5	SA-5b.	Obtains user documentation for the information system, system component, or information system service that describes:	Tested		Pass	X		
SA-5	SA-5b.1.	User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;	Tested		Pass	X		
SA-5	SA-5b.2.	Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and	Tested		Pass	X		
SA-5	SA-5b.3.	User responsibilities in maintaining the security of the system, component, or service;	Tested		Pass	X		
SA-5	SA-5c.	Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;	Tested		Pass	X		
SA-5	SA-5d.	Protects documentation as required, in accordance with the risk management strategy; and	Tested		Pass	X		
SA-5	SA-5e.	Distributes documentation to [Assignment: organization-defined personnel or roles].	Tested		Pass	X		
SA-8	System and Services Acquisition // Security Engineering Principles		Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SA-8		The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SC-11	System and Communications Protection // Trusted Path		Tested	Authentication is not handled by the ECDR app	NA			X
SC-11		The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].	Tested	ECDR provides no security functions	NA			X
SC-13	System and Communications Protection // Cryptographic Protection		Tested	ECDR Does not employ cryptography, nor does it need to.	NA			X
SC-13		The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Tested	ECDR Does not employ cryptography, nor does it need to.	NA			X
SC-18	System and Communications Protection // Mobile Code		Tested	No mobile code is used within the ECDR	NA			X
SC-18		The organization:	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18	SC-18a.	Defines acceptable and unacceptable mobile code and mobile code technologies;	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18	SC-18b.	Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18	SC-18c.	Authorizes, monitors, and controls the use of mobile code within the information system.	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18	System and Communications Protection // Mobile Code		Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SC-18	V-16819	Interview the designer and determine if new mobile code is in development. If no new mobile code is in development, this check is not applicable. 1) If new code is being developed determine and a risk assessment has not been performed, it is a finding.	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18	V-6158	If the application does not send e-mail, this check is not applicable. If the application sends e-mail, ask for user documentation and test results of e-mail portion of application. Additionally, execute the email portion of the application. If possible, configure mail to send to an established email account. If network configurations prevent actual mail delivery, perform the check by examining the mail in the mail queue. Examine documentation and email output. 1) If any email message contains files with the following extensions (.exe, .bat, .vbs, .reg, .jse, .js, .shs, .vbe, .wsc, .sct, .wsf, .wsh), it is a finding.	Tested	ECDR does not send e-mail	NA			X
SC-18	V-6159	The designer will ensure Category 1A mobile code used in an application is signed with a DoD-approved code-signing certificate. The designer will ensure signed Category 1A mobile code used in an application is obtained from a trusted source and is designated as trusted. The designer will ensure Category 1X mobile code is not used in applications. The designer will ensure signed Category 2 mobile code used in an application is signed with a DoD-approved code signing certificate. The designer will ensure Category 2 mobile code not executing in a constrained execution environment is obtained from a trusted source over an assured channel using at least one of the following measures: Interview the application representative and examine the application documentation to determine if Category 1A or 2 mobile code is used.	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The URL of the application must be added to the Trusted Sites zone. This is accomplished via the Tools, Internet Options, and Security Tab. Select the Trusted Sites zone. Click the sites button. Enter the URL into the text box below the Add this site to this zone message. Click Add. Click OK. Note: This requires administrator privileges to add URL to sites on a STIG compliant workstation. Next, test the application. This testing should include functional testing from all major components of the application. If mobile code is in use, the browser will prompt to download the control. At the download prompt, the browser will indicate that code has been digitally signed. 1) If the code has not been signed or the application warns that a control cannot be invoked due to security settings, it is a finding. 2) If the code has not been signed with a DoD approved PKI certificate, it is a finding.						
SC-18	V-6160	If the application does not contain mobile code, this is not applicable. If any mobile code is being transmitted by the application, examine the configuration of the test machine to ensure that no network connections exist. This can be accomplished by typing the netstat command from the command prompt on a Windows client. Ensure that after the mobile code is executed, network connections do not exist. 1) If the application transmits mobile code that attempts to access local operating system resources or establish network connections to servers other than the application server, it is a finding.	Tested	No mobile code is used within the ECDR	NA			X
SC-18	V-6161	Ask the application representative and examine the documentation to determine if the application accepts file inputs via e-mail, ftp, file uploads or other automated mechanisms. If the application does not accept file uploads, this check is not applicable. If the application accepts inputs, investigate the process that is used to process the request. If the process could contain mobile code, a mechanism must exist to ensure that before mobile code is executed, its signature must be validated. The following examples are intended to show determination of the finding:	Tested	ECDR does not accept file inputs	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Non-finding example: The application allows upload of data. The data file is parsed looking for specific pieces of information in an expected format. An application program in accordance with established business rules then processes the data. This situation would be not a finding. Finding example: The application allows upload of data. The data file is sent directly to an execution module for processing. This example could include a .doc file that is sent directly to MS Word for processing. Using this example, if there was a process in place to ensure that the document was digitally signed and validated to be a DoD approved PKI certificate before processing, this would be not a finding.						
SC-18	V-6162	Ask the application representative for design documentation and examine the documentation to determine if additional mobile code types are being used that have not been defined in the mobile code policy. By definition, mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. In order to determine if an emerging technology is covered by the current policy, excerpts of the DoD Mobile Code Policy dated 23 October 2006, and policy memorandum are included so the reviewer knows what types of technologies are included, which he or she must know to determine what is outside the scope of the policy. The memorandum containing the Mobile Code Technologies Risk Category List is available here: https://powhatan.iiie.disa.mil/mcp/mobile-code-memo-2011Mar14.pdf Items covered by the policy include: • ActiveX • Windows Scripting Host when used as mobile code • Unix Shell Scripts when used as mobile code • DOS batch scripts when used as mobile code • Java applets and other Java mobile code	Tested	No mobile code is used within the ECDR	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		• Visual Basic for Applications (VBA) • LotusScript • PerfectScript • Postscript • JavaScript (including Jscript and ECMAScript variants) • VBScript • Portable Document Format (PDF) • Shockwave/Flash • Rich Internet Applications Currently the following are not designated as mobile code by the policy: • XML • SMIL • QuickTime • VRML (exclusive of any associated Java applets or JavaScript scripts) The following are outside the scope of the DoD Mobile Code Policy: • Scripts and applets embedded in or linked to web pages and executed in the context of the web server. Examples of this are Java servlets, Java Server pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side LotusScript. • Local programs and command scripts • Distributed object-oriented programming systems (e.g., CORBA, DCOM). • Software patches, updates, including self-extracting updates - software updates that must be invoked explicitly by the user are outside the mobile code policy. Examples of technologies in this area include: Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins and Linux. If other types of mobile code technologies are present that are not covered by the policy, a written waiver must be granted by the CIO (allowing use of emerging mobile code technology). Also uncategorized mobile code must be submitted for approval. 1) If the application representative is unable to present the written waiver granted by the CIO, it is finding.						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If the application representative provides acceptable written waiver granted by the CIO, it is not a finding.						
SC-18 (2)	System and Communications Protection // Mobile Code | Acquisition / Development/ Use		Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-18 (2)		The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code requirements].	Tested	https://confluence.di2e.net/pages/viewpage.action?pageId=52104691	Pass	X		
SC-2	System and Communications Protection // Application Partitioning		Tested	SAT	Pass	X		
SC-2		The information system separates user functionality (including user interface services) from information system management functionality.	Tested	SAT	Pass	X		
SC-2	System and Communications Protection // Application Partitioning		Tested	Deployed environment is out of scope of this review	NA			X
SC-2	V-16784	Interview the application representative to determine if logical separation exists between application components within the application. Review locations of the components of the application such as web server, database server, and application server. A separate machine is not required but is recommended. Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, and combinations of these methods, or other methods, as appropriate. 1) If the application components are not separated in the application, this is a finding.	Tested	Deployed environment is out of scope of this review	NA			X
SC-2	V-19687	Ask the application representative for a network diagram. Review the network diagram for web servers/web services, web application servers, and database servers. If the application is a tiered web application located in the DoD DMZ and is available to the Internet, verify web servers are on logically separate network segments from the application and database servers. If the application is a tiered web application containing different data types, the application must have physically separate network connections, operating systems and application instances for each data type in the web tier when the application is available to the Internet.	Tested	Deployed environment is out of scope of this review	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		This check does not apply to SIPRNet DMZs or applications that are not available to the Internet. 1) In a tiered DMZ web application with similar data types, if the web server is not on a logically separate network segment from the application and database servers and the application is available to the Internet it is a finding. *Note: Physically separate networks require distinct physical network devices for connections. (e.g. two separate switches or two separate routers)						
SC-2	V-19688	Ask the application representative for a network diagram. Review the network diagram for web servers/web services or any server in the web tier of the DoD DMZ. Verify restricted and unrestricted servers are installed on separate VLANS. 1) If restricted and unrestricted servers in the Web Tier of the DoD DMZ are not installed on separate VLANS, it is a finding. *Note: This check does not apply to SIPRNet DMZs.	Tested	Deployed environment is out of scope of this review	NA			X
SC-2	V-6150	Ask the application representative or examine the application documentation to determine the location of the application code and data. Examine the directory where the application code is located. 1) If the application data is located in the same directory as the code, this is a finding.	Tested	The hosting environment is outside the scope of this evaluation.	NA			X
SC-2 (1)	System and Communications Protection // Application Partitioning | Interfaces For Non-Privileged Users		Tested	SAT	Pass	X		
SC-2 (1)		The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.	Tested		Pass	X		
SC-21	System and Communications Protection // Secure Name / Address Resolution Service (Recursive Or Caching Resolver)		Tested	DDF Security is responsible for communication security	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SC-21		The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Tested	DDF Security is responsible for communication security	Pass		X	
SC-23	System and Communications Protection // Session Authenticity		Tested		Pass		X	
SC-23		The information system protects the authenticity of communications sessions.	Tested	Session Communication Protection Is not handled by the ECDR App	Pass		X	
SC-23 (1)	System and Communications Protection // Session Authenticity | Invalidate Session Identifiers at Logout		Tested		Pass		X	
SC-23 (1)		The information system invalidates session identifiers upon user logout or other session termination.	Tested		Pass		X	
SC-23 (3)	System and Communications Protection // Session Authenticity | Unique Session Identifiers with Randomization		Tested		Pass		X	
SC-23 (3)		The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session identifiers that are system-generated.	Tested		Pass		X	
SC-24	System and Communications Protection // Fail In Known State		Tested		Pass	X		
SC-24		The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	Tested	State management happens either in DDF Kernel or the JAVA virtual machine, not at the Web App Level.	Pass	X		
SC-28	System and Communications Protection // Protection Of Information At Rest		Tested		Pass		X	
SC-28		The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	Tested		Pass		X	
SC-38	System and Communications Protection // Operations Security		Tested	This control should be addressed by the sponsoring Gov't agency	Spons or			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SC-38		The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SC-4	System and Communications Protection // Information In Shared Resources		Tested	The Java Memory Manager manages shared system resources.	NA			X
SC-4		The information system prevents unauthorized and unintended information transfer via shared system resources.	Tested	ECDR does not share system resources.	NA			X
SC-4	System and Communications Protection // Information In Shared Resources		Tested		NA			X
SC-4	V-6142	Ask the application for the design document. Review the design document to ensure the application handles objects so that no residual data exists when reusing objects. No information, including encrypted representations of information, produced by a prior actions is available to any subsequent use of the object. There should be no residual data from the former object. Verify the design document objects which are reused within the application do not contain any residual information. 1) If the design document does not exist or does not address object reuse, it is a finding.	Tested	ECDR does not use objects as defined by this STIG check.	NA			X
SC-4	V-6147	On each computer in the application infrastructure, search the file system for files created or modified in the past week. If the response is too voluminous (more than 200 files), find the files created or modified in the past day. Search through the list for files and identify those that appear to be outside the scope of the application. Ask the application representative how the file relates to the application. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If the creation or modification of the file does not have a clear purpose, it is a finding. The finding details should include the full path of the file. The method described above may not catch all instances of out-of-scope modifications because the	Tested	No files found	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		file(s) may have been modified prior to the threshold date or because the files may be residing on a system other than those examined. If additional information is obtained later in the review regarding improper modification of files, revisit this check. This information may be uncovered when the reviewer obtains more detailed knowledge of how the application works during subsequent checks.						
SC-4	V-6163	Check application to ensure that memory is being released. Also ensure database connections are closed, if applicable. Ask the application representative to demonstrate memory and database connections are released when the application is terminated. 1) If memory is not released and the application is not using garbage collection process for memory (e.g., Java Applications), this is a finding. 2) If the application creates new database connections on entry to the application and does not release them on exit of the application, this is a finding. Ask the application representative to access the application, perform selected actions, and exit the application. Ask the application representative to search for files recently created. For a Windows System: Use Windows Explorer to search for all files (*.*) created today, and then examine the times to narrow the scope of the files to examine. For a Unix System: Enter: # touch -t 200301211020 /tmp/testdatefile The -t flag represents the time option. The time format to be used with -t is {[CC]YYMMDDhhmm[ss]} where the century [CC] and the seconds [ss] are optional fields. The resulting file is: -rw-r--r-- 1 root root 0 Jan 21 10:20 /tmp/testdatefile Enter a second command: # find / -newer /tmp/testdatefile --> This will produce all files on the system with a date later than that of 'testdatefile'.	Tested	Tested with HP Fortify. ECDR does not make database connections. It makes java calls to the DDF Catalog that then communicates with DBs. DDF Catalog is outside of the scope of this evaluation.	Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		# find ./* -newer /tmp/testdatefile --> This will produce all files, recursively, in the current directory with a date later than that of 'testdatefile'. 3) If this list includes temporary files that are not being deleted by the application, this is a finding.						
SC-8	System and Communications Protection // Transmission Confidentiality and Integrity		Tested		Pass		X	
SC-8		The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	Tested		Pass		X	
SC-8	System and Communications Protection // Transmission Confidentiality and Integrity		Tested		Pass		X	
SC-8	V-16785	Ask the application representative for the threat model. Review the threat model for threats regarding session hijacking. Review the threat model for common session hijacking attacks. Examples of session hijacking vulnerabilities can be obtained from the OWASP website. - Predictable session token - Session sniffing - Client-side attacks addressed in APP3580 - MITM attack - Man-in-the-browser attack 1) If the threat model documentation does not address predictable session tokens and provide details regarding the countermeasures taken within the application to mitigate this risk, or if the application representative cannot demonstrate how this risk is mitigated within the application itself, this is a CAT I finding. - Application should utilize a random method of generating session tokens so as to avoid predictable patterns or sequential numbering of session token values. Session identifiers should also utilize the largest character set available to assist randomization. - Application should expire and destroy session identifiers upon logout. - Session identifiers should never be logged. 2) If the threat model documentation does not address session sniffing and provide details regarding the countermeasures taken within the application to mitigate this risk, or if the application	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		representative cannot demonstrate how the risk is mitigated within the application itself, this is a CAT I finding. - Application should set the secure flag when generating cookies that store or transmit session identifiers to ensure values are transmitted via SSL. If the application utilizes URLs with embedded session ids, these URLs can be forwarded in e-mails and e-mail recipients gain access to a system without authentication. Example URL with embedded session id: https://10.10.10.10:443/login.do;jsessionid=F2EE8C97B24635C9995A9D08E69D7B44 3) If URLs containing embedded session ids can be forwarded and used to gain access to the application without authentication, this is a CAT I finding. 4) If the threat model documentation does not address MITM attack, this is a CAT II finding.						
SC-8	V-16794	Ask the application representative to demonstrate the application support mechanisms assuring the integrity of all transmitted information to include labels and security parameters. Ask the application representative to login and demonstrate the application support integrity mechanisms for transmission of both incoming and outgoing files and any transmitted data. For example, hashing/digital signature and cyclic redundancy checks (CRCs) can be used to confirm integrity on data streams and transmitted files. 1) If the application does not support integrity mechanisms for any transmitted data, this is a finding. 2) If the application does not support integrity mechanisms for file transmission, this is a finding. *Note: These checks apply to all data transmitted by REST-styled or SOAP-based Web Services.	Tested		Pass		X	
SC-8	V-19701	If the application does not utilize SOAP messages, this check is not applicable. Ask the application representative for the design document. Review the design document for web services using SOAP messages. Review the design document and verify the message elements Message ID, Service Request, Timestamp and SAML Assertion are signed.	Tested	ECDR does not use SOAP	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		1) If the design document does not exists or does not indicate the entire SOAP messages requiring integrity do not have the appropriate fields, it is a finding.						
SC-8 (1)	System and Communications Protection // Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection		Tested		Pass		X	
SC-8 (1)		The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	Tested		Pass		X	
SC-8 (2)	System and Communications Protection // Transmission Confidentiality and Integrity | Pre-Post Transmission Handling		Tested		Pass		X	
SC-8 (2)		The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Tested		Pass		X	
SI-10	System and Information Integrity // Information Input Validation		Tested	Static Analysis	Pass	X		
SI-10		The information system checks the validity of [Assignment: organization-defined information inputs].	Tested	Static Analysis	Pass	X		
SI-10 (3)	System and Information Integrity // Information Input Validation | Predictable Behavior		Tested	Tested w/ HP Fortify	Pass	X		
SI-10 (3)		The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	Tested	Tested w/ HP Fortify	Pass	X		
SI-11	System and Information Integrity // Error Handling		Tested	Static Analysis	Pass	X		
SI-11		The information system:	Tested	Static Analysis	Pass	X		
SI-11	SI-11a.	Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and	Tested	Static Analysis	Pass	X		
SI-11	SI-11b.	Reveals error messages only to [Assignment: organization-defined personnel or roles].	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SI-16	System and Information Integrity // Memory Protection		Tested		Pass		X	
SI-16		The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.	Tested		Pass		X	
SI-2	System and Information Integrity // Flaw Remediation		Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2		The organization:	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2	SI-2a.	Identifies, reports, and corrects information system flaws;	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2	SI-2b.	Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2	SI-2c.	Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2	SI-2d.	Incorporates flaw remediation into the organizational configuration management process.	Tested	https://di2e-ecdr.atlassian.net/secure/Dashboard.jspa	Pass	X		
SI-2 (2)	System and Information Integrity // Flaw Remediation | Automated Flaw Remediation Status		Tested		NA			X
SI-2 (2)		The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	Tested	No automated vulnerability scanning capability exists to meet this control.	NA			X
SI-2 (3)	System and Information Integrity // Flaw Remediation | Benchmarks for Corrective Actions		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SI-2 (3)		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-2 (3)	SI-2 (3)(a)	Measures the time between flaw identification and flaw remediation; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-2 (3)	SI-2 (3)(b)	Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5	System and Information Integrity // Security Alerts, Advisories, And Directives		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5		The organization:	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5	SI-5a.	Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5	SI-5b.	Generates internal security alerts, advisories, and directives as deemed necessary;	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5	SI-5c.	Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5	SI-5d.	Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5 (1)	System and Information Integrity // Security Alerts, Advisories, And Directives | Automated Alerts and Advisories		Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X
SI-5 (1)		The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
SI-7	System and Information Integrity // Software, Firmware and Information Integrity		Tested	ECDR is released with a PKI digital signature as well as a MD5 and SHA-1 hash	Pass		X	
SI-7		The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].	Tested	ECDR is released with a PKI digital signature as well as a MD5 and SHA-1 hash	Pass		X	
SI-7 (14)	System and Information Integrity // Software And Information Integrity | Binary or Machine Executable Code		Tested	All third-party components within ECDR are licensed and allow access to the source code	Pass			
SI-7 (14)		The organization:	Tested	All third-party components within ECDR are licensed and allow access to the source code	Pass			
SI-7 (14)	SI-7 (14) (a)	Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and	Tested	All third-party components within ECDR are licensed and allow access to the source code	Pass	X		
SI-7 (14)	SI-7 (14) (b)	Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	Tested	No exceptions were required.	Pass	X		
SI-7 (15)	System and Information Integrity // Software And Information Integrity | Code Authentication		Tested	ECDR will be released with a digital signature that would enable this feature if the hosting system or platform has implemented an authentication system.	Pass	X		
SI-7 (15)		The information system implements cryptographic mechanisms to authenticate [Assignment: organization-defined software or firmware components] prior to installation.	Tested	ECDR will be released with a digital signature that would enable this feature if the hosting system or platform has implemented an authentication system.	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
XX-1	Orphaned STIG Checks // Application Security Development		Tested		Pass	X		
XX-1	V-16773	Detailed policy requirements: The Program Manager will provide an Application Configuration Guide to the application hosting providers. The Program Manager will provide a list of all potential hosting enclaves and connection rules and requirements. The Program Manager will ensure development systems, build systems, and test systems have a standardized environment and are documented in the Application Configuration Guide. The Designer will ensure known security assumptions, implications, system level protections, best practices, and required permissions are documented in the Application Configuration Guide. The Designer will ensure deployment configuration settings are documented in the Application Configuration Guide. The IAO will ensure the application is deployed in a manner consistent with the Application Configuration Guide provided by the developers. The Application Configuration Guide is any document or collection of documents used to configure the application. These documents may be part of a user guide, secure configuration guide, or any guidance that satisfies the requirements below: The Application Configuration Guide must be made available to application hosting providers. The Application Configuration Guide will contain a list of all potential hosting enclaves and connection rules and requirements. Development systems, build systems, and test systems must operate in a standardized environment. These settings are to be documented in the Application Configuration Guide. Examples include: • Versions of compilers used • Build options when creating applications and components • Versions of COTS software (used as part of the application) • For web applications, which browsers and what versions are supported All known security assumptions, implications, system level protections, best practices, and required permissions are documented in the Application Configuration Guide.	Tested		Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		All deployment configuration settings are documented in the Application Configuration Guide. Examples include: • Encryptions Settings • PKI Certificate Configuration Settings • Password Settings All deployment configuration settings from the Application Configuration Guide should be implemented. Ask the application representative for Application Configuration Guide or other guidance where these requirements are documented. Verify the configuration settings have been implemented. 1) If any of the above information is missing, or the Application Configuration Guide does not exist, it is a finding. 2) If the settings in the Application Configuration Guide are not implemented, it is a finding.						
XX-1	V-16777	The Program Manager will ensure COTS IA, and IA enabled products, are used to protect sensitive information when the information transits non DoD owned networks, or the system handling the information is accessible by individuals who are not authorized to access the information on the system, comply with NIAP/NSA approved protection profiles. The Program Manager will ensure COTS IA, and IA enabled products, are used to protect classified information when the information transits networks, which are at a lower classification level than the information being transported, comply with NIAP/NSA approved protection profiles. Interview the application representative and determine the IA, and IA enabled COTS products, used in the application. Also, review the confidentiality level for the application. Public releasable data requires a NIAP/NSA approved protection profile for IA, and IA enabled, COTS products. Sensitive data requires a NIAP/NSA approved protection profile for IA, and IA enabled, COTS products. Classified information, when the information transits networks which are at a lower classification level than the information being transported, requires NIAP/NSA approved protection profiles for IA, and IA enabled, COTS products.	Tested	ECDR is not IA or IA-Enabled	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		The accreditation documentation should list the products that are used. A list of validated products and protection profiles is available on the common criteria website: http://www.niap-ccevs.org/cc-scheme/pp/index.cfm 1) Compare that list against the approved products. If any of the third party products are not listed or are below the NIAP/NSA approved protection profiles required by the application, it is a finding.						
XX-1	V-16778	Policy: The Program Manager will obtain DAA approval for all open source, public domain, shareware, freeware, and other software products/libraries with limited or no warranty but are required for mission accomplishment. The designer will document all open source, public domain, shareware, freeware, and other software products/libraries that have limited or no warranty, but which are required for mission accomplishment. Software products and libraries with limited or no warranty will not be used in DoD information systems unless they are necessary for mission accomplishment, and there are no alternative IT solutions available. If these products are required, they must be assessed for information assurance impacts, and must be approved for use by the DAA. Review the DoD policy regarding Open Source Software products: http://www.defenselink.mil/cio-nii/docs/OpenSourceInDoD.pdf Open Source Software: Copyrighted software distributed under a license that provides everyone the right to use, modify, and redistribute the source code of software. Public Domain Software: Software not protected by any copyright laws providing the right to use, modify, and redistribute without permission or payment to the author. Shareware: Copyrighted software distributed under a license that provides a trial right to use and redistribute the binaries. For continued usage, users are required to pay a fee.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Freeware: Copyrighted software distributed under a license that provides a right to use and redistribute the binaries. Unlike shareware, there is no charge for continued use. Commercial Software: Copyrighted software sold for profit by businesses, also referred to as COTS software. 1) If software products (e.g., Open Source Software, Public Domain Software, Shareware and Freeware) and libraries with limited or no warranty are used in DoD information systems except when they are necessary for mission accomplishment and there are no alternative IT solutions available, it is a finding.						
XX-1	V-16779	Verify registration of the application and ports in the Ports and Protocols Database for a production site. 1) If the application requires registration, and is not registered or all ports used have not been identified in the database this is a finding.	Tested		Pass		X	
XX-1	V-16780	Detailed Policy requirements: The Program Manager will ensure all levels of program management receive security training regarding the necessity, impact, and benefits of integrating secure development practices into the development lifecycle. The Program Manager will ensure designers are provided training on secure design principles for the entire SDLC and newly discovered vulnerability types on, at least, an annual basis. The Program Manager will ensure developers are provided with training on secure design and coding practices on, at least, an annual basis. The Program Manager will ensure testers are provided training on at least an annual basis. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Interview the application representative and ask for evidence of security training for application	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		managers, designers, developers, and testers. Examples of evidence include course completion certificates and a class roster. At a minimum, security training should include Security Awareness Training. 1) If there is no evidence of security training, it is a finding.						
XX-1	V-16782	Verify that the organization provides or uses an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource must be an integral part of the organization's incident response capability. This capability is addressed by the DOD CNDSP Program but participation at the organization level must be verified. Interview the application representative to determine if a security incident response process for the application is established. 1) If a security incident response process for the application is not documented, it is a finding. Interview the application representative to determine if a security incident response process contains the following: Identified CNDSP. Reportable incidents are defined. INFCON outlined in the incident response standard operating procedures. A provision exists for user training and annual refresher training. Establishment of an incident response team. Procedure for the plan to be exercised annually. 2) If a security incident response process is not adequate, it is a finding. Interview the application representative to determine if a security incident response process for the application is followed. 3) If a security incident response process for the application is not followed, it is a finding.	Tested	This control should be addressed by the sponsoring Gov't agency	Sponsor			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
XX-1	V-16783	Determine the sensitivity of the data of the application by reviewing the confidentiality levels for which the system was designed. If a traditional review is being conducted at the same time as the application review, this check is not applicable. For sensitive data, the following security guidelines must be followed: • Verify the existence of policy and procedures to ensure the proper handling and storage of information at the site. • Verify system media (e.g., tapes, printouts, etc.) is controlled and the pickup, delivery, receipt, and transfer of system media is restricted to authorized personnel (NIST MP-5). • Verify there is a policy that addresses output handling and retention (NIST SI-12). • Verify policy that addresses output handling and retention is being followed (NIST SI-12). 1) If sensitive data security guidelines do not exist or not followed, it is a finding. For classified data, the following security guidelines must be followed: • Verify the existence of policy and procedures to ensure the proper handling and storage of information at the site. (e.g., end-of-day, security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule). • Verify the existence of a system of security checks at the close of each working day to ensure that the area is secure. • An SF 701: Activity Security Checklist, is required to record such checks. • An SF 702: Security Container Check Sheet, is requires to record the use of all vaults, secure rooms, and containers used for the storage of classified material. • Verify system media (e.g. tapes, printouts, etc.) is controlled and the pickup, delivery, receipt and transfer of system media is restricted to authorized personnel (NIST MP-5). • Verify there is a policy that addresses output handling and retention (NIST SI-12). • Verify policy that addresses output handling and retention is being followed (NIST SI-12). 2) If classified data security guidelines do not exist or are not followed, it is a finding.	Tested	Deployed Environemnt is out of scope of this review	NA			X
XX-1	V-16788	If the application does not implement key exchange, this check is not applicable. Identify all application or supporting infrastructure features using key exchange. Verify the	Tested	ECDR does not implement Key Exchange	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		application is using FIPS-140 validated cryptographic modules for encryption of key exchange algorithms. 1) If the application does not implement encryption for key exchange, it is a finding.						
XX-1	V-16790	If the application does not use a database, this check is not applicable. Ask the application representative how the application authenticates to the database. 1) If the application authenticates to the database by using a database account that has database administrator access, it is a finding.	Tested	ECDR does not use a database	NA			X
XX-1	V-16791	If the application is not a transaction based application that stores and retrieves data, this check is not applicable. Ask the application representative if the application uses a database to store information. If the application utilizes Oracle, SYBASE, or Microsoft SQL Server, then support for journaling and rollback is already present in the tools. Note: Microsoft Access does not support journaling and rollback. If Microsoft Access is used, ask the application representative to demonstrate the rollback and journaling features of the application. 1) If the application representative cannot demonstrate support for journaling and rollback, it is a finding.	Tested	ECDR is not a transaction based system	NA			X
XX-1	V-16792	If the application does not contain sensitive or classified information this check does not apply. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable.. Ask the application representative to review global variables for the application. If the global variables contain sensitive information, ask the application representative if they are required to be encrypted by the data owner. If the data is required to be encrypted by the data owner, ask the application representative to demonstrate they are encrypted.	Tested	ECDR does not contain sensitive data	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Note: The .Net Framework 2.0 and higher provides a SecureString class which can encrypt sensitive string values. 1) If sensitive or classified information is required to be encrypted by the data owner and global variables containing sensitive information are not encrypted, it is a finding.						
XX-1	V-16793	If the application does not contain sensitive or classified information this check is not applicable. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Ask the application representative to demonstrate how the application clears and releases memory blocks. Microsoft Visual C++ provides SecureZeroMemory that will not be optimized out of code for clearing sensitive and classified data. 1) If the application releases objects before clearing them, it is a finding.	Tested	ECDR does not contain sensitive data	NA			X
XX-1	V-16796	Ask the application representative to demonstrate that passwords are encrypted before they are transmitted. 1) If the application does not use passwords for identification and authentication, this check is not applicable. 2) If the application does not encrypt passwords before transmitting them, it is a finding.	Tested	ECDR does not transmit passwords	NA			X
XX-1	V-16820	The CM repository access permissions are not reviewed at least every three months. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Ask the application representative when the last time the access privileges were reviewed. 1) If access privileges were reviewed within the last three months, this is not a finding.	Tested	The development team consists of 3 people. Any change in the team is immediately known and appropriate actions would be taken. Althouh not completely NA, this STIG check is not very appropriate for a development effort of this size.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
XX-1	V-16827	Ask the application representative to provide tests plans, procedures and results to ensure system initialization, shutdown, and aborts keep the system in a secure state. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. 1) If test plans, procedures, and results do not exist ,or at least executed annually, it is a finding.	Tested	ECDR does not transition states	NA			X
XX-1	V-16834	If a DoD STIG or NSA guide is not available, application and application components will be configured by the following in descending order as available: (1) commercially accepted practices, (2) independent testing results, or (3) vendor literature. 1) If the application and application components do not have DoD STIG or NSA guidance available and not configured by (1) commercially accepted practices, (2) independent testing results, or (3) vendor literature, it is a finding.	Tested	Deployed environment is out of scope of this review	NA			X
XX-1	V-16840	Examine the system to determine if an automated, continuous on-line monitoring and audit trail creation capability is present with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected. 1) If this monitoring capability does not exist, it is a finding.	Tested		Pass		X	
XX-1	V-16842	Interview the application representative and review the SOPs to ensure that violations of IA policies are analyzed and reported. 1) If there is no policy reporting IA violations, it is a finding.	Tested	Deployed environment is out of scope of this review	NA			X
XX-1	V-16843	Interview the application representative and determine if any logs are being automatically monitored and if alerts are sent out on any activities. 1) If there are no automated alerts, this is a finding.	Tested		Pass		X	

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
XX-1	V-16844	Verify that a licensed copy of the operating system software and other critical software is in a fire rated container or stored separately (offsite) from the operational software. 1) If operating system software and other critical software is not in a fire rated container, or stored offsite, it is a finding.	Tested	Deployed environment is out of scope of this review	NA			X
XX-1	V-16845	Validate that backup and recovery procedures incorporate protection of the backup and restoration assets. Verify assets housing the backup data (e.g., SANS, tapes, backup directories, software) and the assets used for restoration (e.g., equipment and system software) are included in the backup and recovery procedures. 1) If backup and restoration devices are not included in the recovery procedures, it is a finding.	Tested	ECDR has no data to backup	NA			X
XX-1	V-16846	All applications should document disaster recovery procedures to include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance. Ask the application representative to review these plans. For MAC 1 applications, verify the disaster plan exists and provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. For MAC 2 applications, verify the disaster plan exists and provides for the resumption of mission or business essential functions within 24 hours activation. For MAC 3 applications, verify the disaster plan exists and provides for the partial resumption of mission or business essential functions within 5 days of activation. 1) If the disaster plan does not exist or does not meet the MAC level requirements, this is a finding.	Tested	A DRP is not applicable to software developer	NA			X
XX-1	V-16849	Ask the application representative if a group of users share login information to the system. 1) If an account that belongs to a group that can login to the system, this is a finding.	Tested	ECDR does not manage authentication	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		2) If there is a login shared by more than one user, this is a finding.						
XX-1	V-16850	Interview the application representative and determine if the application is publicly accessible. 1) If the application is publicly accessible and traffic is not being routed through a DMZ, it is a finding.	Tested	The hosting environment is outside the scope of this evaluation	NA			X
XX-1	V-19699	If the application does not utilize UDDI registries, this check is not applicable. Ask the application representative to demonstrate web service inquiries to UDDI provide read-only access to the registry for anonymous users. 1) If application representative is unable to demonstrate web service inquiries to UDDI provide read-only access to the registry for anonymous users, it is a finding.	Tested	ECDR does not use UDDI registries	NA			X
XX-1	V-19700	If the application does not utilize UDDI registries, this check is not applicable. Ask the application representative to demonstrate authentication is required when UDDI registry contains sensitive information. 1) If the application representative is unable to demonstrate authentication is required when UDDI registry contains sensitive information, it is a finding.	Tested	ECDR does not use UDDI registries	NA			X
XX-1	V-22031	Examine the contents of a SOAP message using a SessionIndex in the SAML element AuthnStatement. Verify the information which is tied to the SessionIndex. If the SessionIndex is tied to privacy information, and it is not encrypted, it is a finding.	Tested	ECDR does not process SOAP or SAML	NA			X
XX-1	V-47163	Ask the application representative to demonstrate their cryptographic hash validation process or provide process documentation. The validation process will vary based upon the operating system used as there are numerous clients available that will display a file's cryptographic hash for validation purposes. Linux operating systems include the "sha256sum" utility. For Linux systems using sha256sum command syntax is: sha256sum [OPTION]... [FILE]...	Tested	ECDR does not validate hashes	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Windows does not natively provide a SHA256 checksum validation tool; however, there are utilities available that provide this capability. A validation process involves obtaining the application files' cryptographic hash value from the programs author or other authoritative source such as the application's web site. A utility like the "sha256sum" utility is then run using the downloaded application file name as the argument. The output is the files' hash value. The two hash values are compared and if they match, then file integrity is ensured. If the application being reviewed is a COTS product and the vendor used a SHA1 or MD5 algorithm to generate a hash value, this is not a finding. If the application being reviewed is a COTS product and the vendor did not provide a hash value for validating the package, this is not a finding. If the integrity of the application files/code is not validated prior to deployment to DoD operational networks, this is a finding.						
XX-1	V-6135	The designer will ensure: - NIST-certified cryptography is used to protect stored sensitive information if required by the information owner. - NIST-certified cryptography is used to store classified non-Sources and Methods Intelligence (SAMI) information if required by the information owner. - A classified enclave containing SAMI data is encrypted with NSA-approved cryptography. Review the system security plan or interview the application representative to determine the classification of data in the application. Also, review encryption mechanisms protecting the data. This should include all data stored by REST-Style or SOAP-based web services. NIST-certified cryptography should be used to protect stored sensitive information if required by the information owner. NIST-certified cryptography should be used to protect stored classified non-SAMI data if required by the information owner.	Tested	There is no sensitive information within the ECDR	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		NSA-approved cryptography should be used to protect stored classified SAMI information. 1) If data at rest is not protected with the appropriate level of encryption, this is a finding.						
XX-1	V-6136	Policy: The designer will ensure unclassified, sensitive data transmitted through a commercial or wireless network is protected using NIST certified cryptography. The designer will ensure classified data, transmitted through a network that is cleared to a lower level than the data being transmitted, is separately protected using NSA approved cryptography. The designer will ensure data in transit through a network at the same classification level, but which must be separated for need to know reasons, is protected minimally with NIST certified cryptography. The designer will ensure SAMI data in transit through a network at the same classification level is protected with NSA approved cryptography. Interview the application representative to determine if sensitive data is transmitted over a commercial circuit or wireless network (e.g., NIPRNet, ISP, etc.). 1) If any sensitive data is transferred over a commercial or wireless network and is not encrypted using NIST FIPS 140-2 validated encryption, this is a CAT I finding. Interview the application representative to determine if classified data is transmitted over a network cleared to a lower level than the data. (e.g., TS over SIPRNet, Secret over NIPRNet, etc.). 2) If classified data is transmitted over a network cleared to a lower level than the data and NSA approved type-1 encryption is not used to encrypt the data, this is a CAT I finding. Interview the application representative and determine if the data in transit must be separated for need to know reasons.	Tested	The hosting environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		3) If data in transit across a network at the same classification level is separated for need-to-know reasons and the data is not minimally encrypted using NIST FIPS 140-2 validated encryption, this is a CAT II finding. Interview the application representative and determine if SAMI data is transmitted. 4) If SAMI data in transit across a network at the same classification level is not separately encrypted using NSA type-1 approved encryption, this is a CAT II finding. *Note: These checks apply to all data transmitted by REST-styled or SOAP-based Web Services.						
XX-1	V-6137	If the application does not utilize encryption, key exchange, digital signature, or hash, FIPS 140-2 cryptography is not required and this check is not applicable. Identify all application or supporting infrastructure features that require cryptography such as, file encryption, VPN, SSH, etc. Verify the application is using FIPS-140 validated cryptographic modules. The National Institute of Standards and Technology's FIPS 140-1 and FIPS 140-2 Vendor List is located at: http://csrc.nist.gov/cryptval/. 1) If the application requiring encryption, key exchange, digital signature or hash is using an unapproved module or no module, it is a finding. 2) If the application utilizes unapproved modules for cryptographic random number generation, it is a finding. Note: If the application uses WS Security tokens, W3C XML Signature can be used to digitally sign messages and provide message integrity.	Tested	ECDR does not implement any cryptography.	NA			X
XX-1	V-6138	MAC I or DoD Information Systems processing classified information, require the following events and data for auditing. Types of events are: - Successful and unsuccessful attempts to access security files. - Successful and unsuccessful logons.	Tested	ECDR provides none of the capabilities that require auditing.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		- Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Possible use of covert channel mechanisms. - Privileged activities and other system-level access. - Starting and ending time for access to the system. - Security relevant actions associated with periods processing or the changing of security labels or categories of information. - Deletion or modification of data. Audit records include: - User ID - Date and time of the event - Type of event - Success or failure of event - origin of request (e.g., originating host's IP address) for Identification and Authentication events only - name of data object modified or deleted for deletion or modification events only - reason user is blocked or blacklisted for blocking or blacklisting events only - Data required to monitor for the possible use of covert channels events only MAC II DoD Information Systems processing sensitive information require the following events and data for auditing. Types of events are: - Successful and unsuccessful attempts to access security files. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port. - Activities that might modify, bypass, or negate safeguards controlled by the system. - Deletion or modification of data. Audit records include: - User ID - Date and time of the event						

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		- Type of event - Success or failure of event - origin of request (e.g., originating host's IP address) for Identification and Authentication events only - name of data object modified or deleted for deletion or modification events only - reason user is blocked or blacklisted for blocking or blacklisting events only MAC III or DoD Information Systems processing publicly released information require the following events and data for auditing. Types of events are: - Successful and unsuccessful attempts to access security files. - Deletion or modification of data Audit records include: - User ID - Date and time of the event - Type of event - origin of request (e.g., originating host's IP address) for Identification and Authentication events only. - name of data object modified or deleted for deletion or modification events only 1) If all the required events and associated details are not included in the log or there is not a logging mechanism, it is a finding. *Note: The mechanism that performs auditing may be a combination of the operating system, web server, database, application, etc. Also web services may be distributed over many geographic locations; however, auditing requirements remain the same in web services as they do in a traditional application.						
XX-1	V-6139	Examine the application documentation and ask the application representative what automated mechanism is in place to ensure the administrator is notified when the application logs are near capacity. 1) If an automated mechanism is not in place to warn the administrator, it is a finding.	Tested	Audit management is handled by the hosting platform	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		If the application representative or the documentation indicates a mechanism is in place, examine the configuration of the mechanism to ensure the process is present and executing. 2) If an automated mechanism is not executing, it is a finding. Note: This may be automated by the operating system of the application servers.						
XX-1	V-6143	Identify the application user account(s) that the application uses to run. These accounts include the application processes (defined by Control Panel Services (Windows) or ps –ef (UNIX)) or for an n-tier application, the account that connects from one service (such as a web server) to another (such as a database server). Determine the user groups in which each account is a member. List the user rights assigned to these users and groups and evaluate whether any of them are unnecessary. 1) If the rights are unnecessary, it is a finding. 2) If the account is a member of the Administrators group (Windows) or has a User Identification (UID) of 0 (i.e., is equivalent to root in UNIX), it is a finding. 3) If this account is a member of the SYSAdmin fixed server role in SQL Server, it is a finding. 4) If the account has DDL (Data Definition Language) privileges (create, drop, alter), or other system privileges, it is a finding. Search the file system to determine if these users or groups have ownership or permissions to any files or directories. Review the list of files and identify any that are outside the scope of the application. 5) If there are such files outside the scope of the application, it is a finding. Check ownership and permissions; identify permissions beyond the minimum necessary to support the application.	Tested	ECDR requies no additional user accounts	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		6) If there are instances of unnecessary ownership or permissions, it is a finding. The finding details should note the full path of the file(s) and the associated issue (i.e., outside scope, permissions improperly granted to user X, etc.). 7) If the target is a .NET application that executes with least privileges using code access security (CAS), this is not a finding.						
XX-1	V-6146	Before actual testing, determine which application functions to examine, giving preference to report generation capabilities and the most common user transactions that involve sensitive data (FOUO, secret or above). Ask the application representative for the application's classification guide. This guide should document the data elements and their classification. Logon to the application and perform these in sequence, printing output when applicable. The application representative's assistance may be required to perform these steps. For each function, note whether the appropriate markings appear on the displayed and printed output. If a classification document does not exist, data must be marked at the highest classification of the system. Appropriate markings for an application are as follows: For classified data, markings are required at a minimum at the top and the bottom of screens and reports. For FOUO data, markings are required at a minimum of the bottom of the screen or report. In some cases, technology may prohibit the appropriate markings on printed documents. For example, in some cases, it is not possible to mark all pages top and bottom when a user prints from a browser. If this is the case, ask the application representative if user procedures exist for manually marking printed documents. If procedures do exist, examine the procedures to ensure that if the users were to follow the procedures the data would be marked correctly. Also, ask how these procedures are distributed to the users. 1) If appropriate markings are not present within the application and it is technically possible to have the markings present, it is a finding. 2) If it is not technically feasible to meet the minimum marking requirement and no user procedures exist or if followed the procedures will result in incorrect markings, or the procedures are not readily available to users, it is a finding.	Tested	ECDR has no sensitive data	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		In any case of a finding, the finding details should specify which functions failed to produce the desired results. After completing the test, destroy all printed output using the site's preferred method for disposal. For example: utilizing a shredder or disposal in burn bags. Note: Physical markings on hardware do not meet this requirement.						
XX-1	V-6154	Policy: The designer will ensure the application is organized by functionality and roles to support the assignment of specific roles to specific application functions. The IAO will ensure access to privileged accounts is limited to privileged users. The IAO will ensure non-privileged accounts are limited to non-privileged users. The IAO will ensure the application account is established and administered in accordance with a role based access scheme to enforce least privilege and separation of duties. Check: Log on as an unprivileged user. Examine the user interfaces (such as, graphical, web, and command line) to determine if any administrative functions are available. Privileged functions include the following: • Create, modify, and delete user accounts and groups • Grant, modify, and remove file or database permissions • Configure password and account lockout policy • Configure policy regarding the number and length of sessions • Change passwords or certificates of users other than oneself • Determine how the application will respond to error conditions • Determine auditable events and related parameters • Establish log sizes, fill thresholds, and fill behavior (i.e., what happens when the log is full) Some applications may only contain administrator access and no other access. For example, network appliances may have administrator only access. Web applications with no user	Tested	ECDR is too small and simple to assign roles	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		authentication required are also considered to contain a single role, unless the web application provides administrative access to publish web server content. 1) If the application is designed specifically to only have one role, this check is not applicable. 2) If non-privileged users have the ability to perform any of the functions listed above, it is a finding. Finding details should specify which of the functions are not restricted to privileged users. Work closely with the application SA before testing any administrative changes to ensure local change management procedures are followed. Immediately back out of any changes that occur during testing. Review administrative rights assignments in all application components, including the database software and operating system. On Windows systems, review each of the User Rights to determine which users and groups are given more than default capabilities. User Rights can be viewed by using DumpSec, then selecting Reports, Dump Rights. 3) If privileged rights are granted to non-privileged users, it is a finding. *Note: Web services are required to separate functionality by roles.						
XX-1	V-6167	The design of the application should account for the following: 1) Connections to databases are left open 2) Access control mechanisms are disabled. 3) Data left in temporary locations. Testing application failure will require taking down parts of the application. Examine application test plans and procedures to determine if this type of failure was tested. If test plans exist, validate the tests by performing a subset of the checks. If test plans do not exist, an application failure must be simulated. Simulate a failure. This can be accomplished by stopping the web server service and/or the database service. Also, for applications using web services, stop the web service and/or the database. Check to ensure that application data is still protected. Some examples of tests follow. Try to submit SQL queries to the database. Ensure that the database requires authentication before	Tested	ECDR performs none of the functions of this check	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		returning data. Try to read the application source files; access should not be granted to these files because the application is not operating. Try to open database files; data should not be available because the application is not operational. 1) If any of these tests fail, it is a finding.						
XX-1	V-6169	All application ports, protocols, and services needed for application operation need to be in compliance with the DoD Ports and Protocols guidance. Check (http://iase.disa.mil/ports/index.html) to ensure the ports, protocols, and services are in compliance with the PPS CAL. Check all necessary ports and protocols needed for application operation (only those accessed from outside the local enclave) are checked against the DoD Ports and Protocols guidance to ensure compliance. Identify the ports needed for the application: • Look at System Security Plan/Accreditation documentation • Ask System Administrator • Go to Network Administrator Retina Scanner • Go to Network Reviewer • If a network scan is available, use it • Use netstat/task manager • Check /etc/services 1) If the application is not in compliance with DoD Ports and Protocols guidance, it is a finding.	Tested	https://confluence.di2e.net/display/ECDR/Ports%2C+Protocols%2C+and+Services	Pass	X		
XX-1	V-6170	List all IA or IA enabled products that are part of the application. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) / Common Criteria Evaluated Products. 1) If the products have not been evaluated or are in the process of being evaluated, it is a finding.	Tested	ECDR has no IA or IA-Enabled components	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		According to NSTISSP 11, an IA enabled product is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. To meet the intent of NSTISSP 11, acquired IA enabled products must be evaluated if the IA features are going to be used to perform one of following security services: availability, integrity, confidentiality, authentication, or non-repudiation. Therefore, the determination of whether an IA enabled product must be evaluated will be dependent upon how that particular product will be used within the consumer's system architecture. Examples of such products include security enabled web browsers, screening routers, and security enabled messaging systems. Although NSTISSP 11 uses both terms, the policy as stated applies equally to both types of products. A list of certified products is available on the common criteria website: http://www.commoncriteriaportal.org/products.html Below are definitions of IA and IA enabled products from DoD Instruction 8500.2. IA Product - Product or technology whose primary purpose is to provide security services e.g., confidentiality, authentication, integrity, access control or non-repudiation of data; correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices. IA Enabled Product - Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.						
XX-1	V-6171	Ensure that a disaster recovery plan is in place for the application. If the application is part of the site's disaster recovery plan, ensure that the plan contains detailed instructions pertaining to the application. Ensure that recovery procedures indicate the steps needed for secure recovery. 1) If a disaster recovery plan does not exist or the application is not part of the site's disaster recovery plan, it is a finding.	Tested	The hosting environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		Verify that the recovery procedures include any special considerations for trusted recovery. 2) If any special considerations for trusted recovery are not documented, it is a finding.						
XX-1	V-6172	Check the following based on the MAC level of the application. For MAC 3 applications: Validate backup procedures exist and are performed at least weekly. A sampling of system backups should be checked to ensure compliance with the control. For MAC 2 applications: Validate backup procedures exist and are performed at least daily. Validate recovery media is stored at an off-site location and ensure the data is protected in accordance with its mission assurance category and confidentiality level. This validation can be performed by examining an SLA or MOU/MOA that states the protection levels of the data and how it should be stored. A sampling of system backups should be checked to ensure compliance with the control. Verify that the organization tests backup information to ensure media reliability and information integrity. Verify that the organization selectively uses backup information in the restoration of information system functions as part of annual contingency plan testing. For MAC 1 applications: Validate that the procedures have been defined for system redundancy and they are properly implemented and are executing the procedures. Verify that the redundant system is properly separated from the primary system (i.e., located in a different building or in a different city). This validation should be performed by examining the secondary system and ensuring its operation. Examine the SLA or MOU/MOA to ensure redundant capability is addressed. Finding details should indicate the type of validation performed. Examine the mirror capability testing procedures and results to insure the capability is properly tested at 6	Tested	The hosting environment is outside the scope of this evaluation	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		month minimum intervals. 1) If any of the requirements above for the MAC level of the application are not met, it is a finding.						
XX-1	V-6173	Ensure a process is in place to retain application audit log files for one year and five years for SAMI data. 1) If audit logs have not been retained for one year or five years for SAMI data, this is a finding.	Tested	The hosting environment is outside the scope of this evaluation	NA			X
XX-1	V-6174	Ask if any database exports from this database are imported to development databases. If no database exports exist, this check is not applicable. If there are such exports, ask if policy and procedures are in place to require the modification of the production database account passwords after import into the development database. 1) If there are no policy and procedures in place to modify production database account passwords, it is a finding. If there are such exports, ask if the production database includes sensitive data identified by the data owner as sensitive such as passwords, financial, personnel, personal, HIPAA, Privacy Act, or classified data is included. 2) If any database exports include sensitive data and it is not modified or removed prior to or after import to the development database, it is a finding. 3) If there are no policy and procedures in place to modify production database account passwords, it is a finding. If there are such exports, ask if the production database includes sensitive data identified by the data owner as sensitive such as financial, personnel, personal, HIPAA, Privacy Act, or classified data is included.	Tested	ECDR does not use a database.	NA			X

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		4) If any database exports include sensitive data, and it is not modified or removed prior to or after import to the development database, it is a finding.						
XX-1	V-6198	The application and the application client (e.g., web browser, C++ application, etc.) must be designed to work on a STIG compliant platform. Vulnerabilities are discovered frequently and security updates must be applied constantly and may not be reflected in the latest baseline of a secure image of the operating system. Any finding required to make the application client operate correctly will be documented in this check. Conduct a review of the application and the application client platform using the SRR process or utilize an up to date application/client platform SRR if available. Ensure the application client platform was included in the overall application SRR review. Ensure the SRR was completed after the most recent system updates or changes. If the client is Windows based and the application uses either a browser interface or an MS Office Product, a Desktop Application review must also be conducted. 1) If the review of the application client platform produces findings indicating that the application client will not operate correctly in a STIG compliant environment, it is a finding. Ensure the application review includes test and build systems. All deployment, development, as well as test and build systems should be included in the application review to ensure the applicable DoD approved or other acceptable security configuration documents have been applied. 2) If the application review does not include all deployment, development, as well as test and build systems, it is a finding.	Tested	Tested SAT	Pass	X		
XX-1	V-7013	Ask the application representative for the design document for the application. Review the design document. If the application is a COTS/GOTS product or is composed of only COTS/GOTS products with no custom code, this check does not apply unless the application is being reviewed by or in conjunction with the COTS/GOTS vendor in which case this check is applicable. Examine the design document and/or the threat model for the application and verify the following information is documented: -- All external interfaces.	Tested	See the Threat Model and Architecture	Pass	X		

Control	Number	Description	Test Status	Dev Notes	Test Result	Impl	Interop	No-Capabilit
		-- The nature of information being exchanged. -- Any protections on the external interface. -- User roles required for access control and the access privileges assigned to each role. -- Unique security requirements (e.g., encryption of key data elements at rest). -- Categories of sensitive information processed by the application, and their specific protection plans (e.g., PII, HIPAA). -- Restoration priority of subsystems, processes, or information. -- Verify the organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail. 1) If the design document is incomplete, it is a finding.						