ENCLAVE TEST AND DEVELOPMENT SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 3

22 January 2016

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Enclave Test & Development (T&D) Security Technical Implementation Guides (STIGs) provide the information protection guidance necessary to ensure secure implementation of Information Systems (ISs) and networks providing test and development services. These STIGs provide guidance for the separation of network traffic, functionality, and supplement existing security requirements already levied against test and development systems. Networks not directly connected to the Defense Information Systems Network (DISN) (e.g., Defense Research and Engineering Network (DREN)) are currently outside the scope of this document. These networks must follow a pre-established connection approval process, which is available from the Department of Defense (DoD) Chief Information Officer's (CIO) office or the network owner.

DoD ISs must have adequate safeguards, both technical and procedural, to ensure the security of data processed within these environments. In general, DoD ISs must provide feasible safeguards to achieve the highest level of security possible. The actual safeguards used will be commensurate with the operational requirements, information sensitivity level, and consequences of exploitation of the specific test and development environment established.

A majority of DoD ISs typically connects to Local Area Networks (LANs) and use Wide Area Networks (WANs) (e.g., the Non-Classified Internet Protocol Router Network [NIPRNet] and the Secret Internet Protocol Router Network [SIPRNet]) as the primary data transport mechanism. Due to the flexibility needed for these agile environments, providing an adequate level of protection at an acceptable cost is difficult in this type of environment. This document is aimed at identifying mitigating controls to aid in securing and protecting the test and development environmental boundaries and the data being tested or developed, while achieving the objectives identified in the DoD Directive, "Information Assurance, 8500.1" and the Department of Defense Instruction, "Information Assurance (IA) Implementation, 8500.2".

This document applies to both DoD- and contractor-managed (developing on behalf of the DoD) test and development environments, unless otherwise excluded. The requirements within the Test and Development STIGs are designed to assist Authorizing Officials (AOs), Information Systems Security Managers (ISSMs), Information Systems Security Officers (ISSOs), and System Administrators (SAs) in performing necessary risk assessments for protecting DoD network infrastructures and testing and development data (e.g., source code). This document will assist in identifying external security exposures created when connecting the organization to one or more information systems outside the organization's control. The scopes of these STIGs are specifically for environments used in testing, development of applications, and network infrastructure that will be deployed to either the NIPRNet or SIPRNet. Research, development, testing, and evaluation of Platform IT are not included in the scope of this document.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD

cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), STIGs, and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6   Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DoD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. TEST AND DEVELOPMENT ZONE PARAMETERS

One of the most challenging aspects of requirements building for test and development environments is defining the terminology. Technical experts have differing opinions as to what "test" and "development" actually mean and what security controls need to be in place to protect not only those systems, but also the systems they may connect to or otherwise associate with. This section provides basic terminology used in the Enclave T&D STIG.

Testing is the process used to help identify the correctness, completeness, security, and quality of developed computer software. Testing is a process of technical investigation intended to reveal quality-related information about the product with respect to the context in which it is intended to operate. This includes, but is not limited to, the process of executing a program or application with the intent of finding errors. Testing may include installation of patches or software to see if the change "breaks" a system or application, testing the validity of certain controls, or testing the functionality of the application. Some testing cycles may require building and rebuilding applications or operating systems on a continual basis.

There may be many levels of testing, such as end state testing, directly preceding production status. End state testing refers to those systems that are prepared for production environments from an operational and security perspective. This type of testing will have different security requirements from that of the initial test phase.

Development is the process by which something passes by degrees to a different stage (particularly a more advanced or mature stage); software development is the process of designing, writing, testing, and maintaining the source code of computer programs. Software development may include new development, modification, reuse, re-engineering, maintenance, or any other activities that result in software products. The definition includes many phases of the development lifecycle. The Application Security and Application Services Checklists define security requirements for development. Program of Record (POR) systems that develop applications or software must be IA-compliant prior to deployment on operational networks.

3. TEST AND DEVELOPMENT ENVIRONMENTS (ZONES)

T&D zones, for the purposes of this document, identify four elements, which are architecture, remote access, development, and testing and evaluation. In order to isolate and segregate differing security environments, a zone breakdown has been developed to establish the security baselines, which must be in place for each test and development environment.

The architectural component describes policy and placement of network infrastructure to ensure security of the agile environments. The proper architecture must be in place to safeguard such things as the application source code and test data containing sensitive information. A new concept for the STIGs is the allowance for temporary connections to operational live data for testing scenarios that cannot otherwise be tested. Due to the risk involved with using live DoD data, the ISSM must work in conjunction with the AO to determine what may be tested in the operational environment. All zones must be documented and the infrastructure certified with an Interim Approval to Operate (IATO) prior to connection to any external network (e.g., DISN, Internet, other non-DoD network). Proper care to separate network segments using logical or physical separation is required where necessary. Network segments designated for development where secure systems are present must not interact with non-IA-compliant network segments used for general application and product testing. Building a secure infrastructure will minimize the risk of theft and corruption of source code either accidentally or maliciously. Remote access capabilities described for each zone environment is crucial for testers and developers to access the appropriate tools needed to do their job while maintaining the proper physical and/or logical separation.

Development of applications is the most important aspect of the T&D environments. Securing the source code needs to be the highest priority prior to migration into a live operational network. Compromise of the code can cause integrity and availability issues if proper vetting is not complete prior to migration. Vetting will take place through strict Control Change Management (CCM) processes developed by the organization. Along with the CCM processes, all application code must go through proper testing and an application code review to mitigate potential issues. Applications development must also follow the proper IA controls and security requirements using the Application Security Development (ASD) STIG.

One method of testing applications typically requires a control set of data that will have predetermined outcomes. These control sets should be kept in a secure manner so the integrity of the data is not compromised. Data needed for testing from a DoD operational network must be sanitized for any sensitive material such as personal information or data exempted under the Freedom of Information Act. Any data tested against applications in any of the zone environments will be sanitized accordingly.

Downloading data to be used in a T&D environment through a secure perimeter from an untrusted network or website is mandatory. Bringing data directly from an untrusted network or downloaded from a personal computer or home Internet connection must be prohibited. Scanning data is crucial to ensure the integrity of the information prior to deployment for testing and development processes. While not an all-inclusive list, data in this situation includes OS patches, application updates, Operating Systems, development tools, and test data. In the

environment, there will typically be one or more IA-compliant systems accessing a secure Internet connection. If a secure internet connection is not available, such as zone D, a connection in another zone can be used to download data and sneaker-netted using approved physical media. Scanning the data with an antivirus program will reduce the risk of exploits and taking over vulnerable systems in the test and development environment. Downloading data from a single workstation for all zone environments is acceptable. Organizations with NIPRNet connections must download all data through their NIPRNet connection for scanning at the IAPs. Contractors or other DoD organizations without any direct NIPRNet connectivity will need to use a secure Internet connection following all applicable DoD IA policy and STIG requirements.

A high-level overview of how each test and development environment may potentially be engineered is provided below in Figure 3-1, which incorporates the use of all zones. The remaining subsections detail each zone and the requirements for network connectivity and IA compliancy.

Figure 3-1: Example Zone Architecture
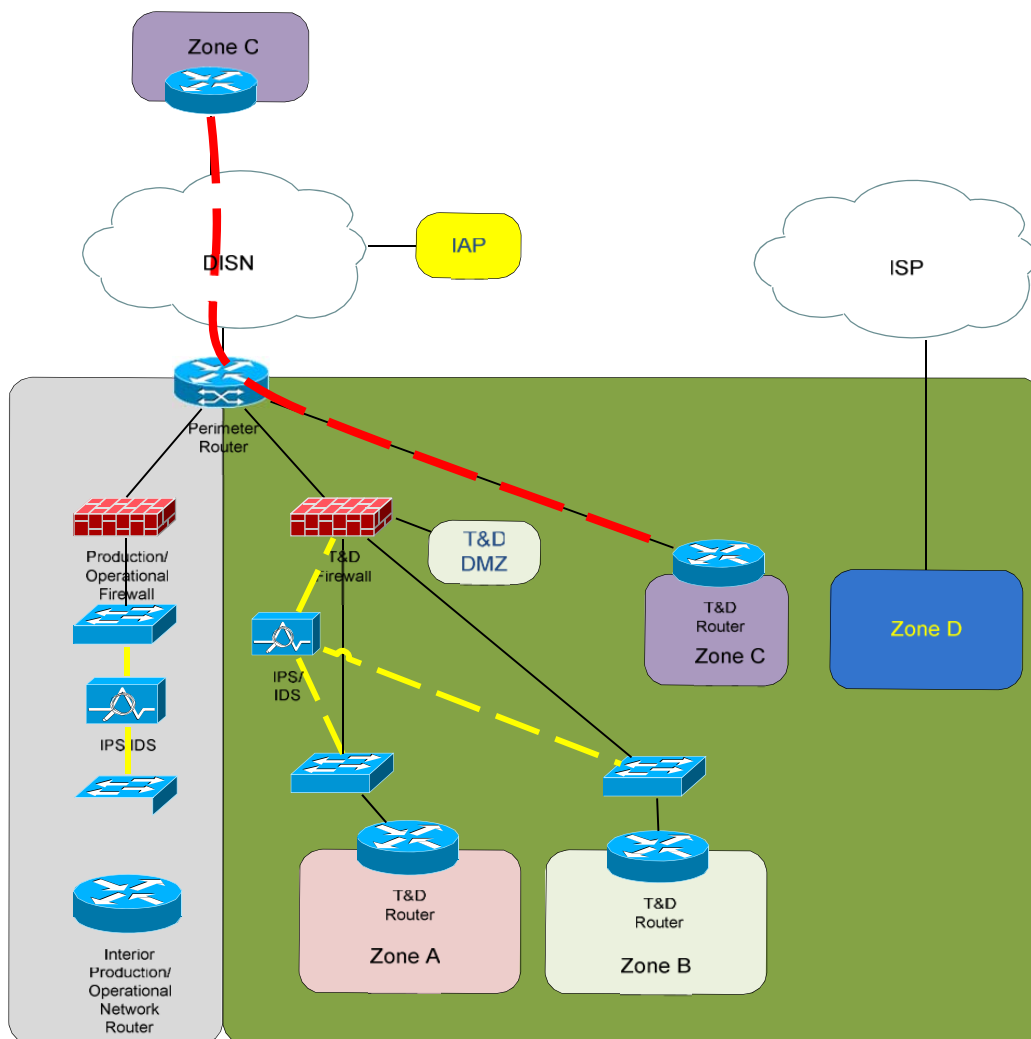
3.1 Zone A Environment

The Zone A environment is typically configured as a mirrored operational network for final end stage testing. This environment will have connectivity to the live operational network for final data testing prior to the product or application deployment into the operational network.

Since the Zone A environment mimics the operational network, the supporting infrastructure will comply with all applicable DoD policy and security requirements. Prior to being granted connectivity, it will go through a risk assessment for the Connection Approval Process. The environment is required to hold at minimum, an IATO for connectivity to the DISN or other live operational network within the DoD. An Interim Authority to Test (IATT) may be obtained where the test environment requires testing of live operational data that cannot be mirrored or make use of sanitized data. The ISSM will conduct a security risk assessment for the requested IATT approved by the AO.

If a requirement exists for remote access into the T&D environment, a Virtual Private Network (VPN) solution must be in place. VPNs in use must terminate in the T&D Demilitarized Zone (DMZ) prior to traffic entering the environment for proper traffic inspection. VPNs must take proper measures to secure the tunneled connections with the use of approved encryption mechanisms and standards for the sensitivity level or classification of data in use. Unclassified need-to-know data must use FIPS 140-2 validated cryptographic modules and classified data must use NSA-approved encryption. VPNs initiated from systems outside of the T&D environment must not allow access to the local system's network while connected. VPN must not use split tunneling during connection to the environment.

Development within the environment should be minimal for final revisions and minor updates of products in the final testing phase. While all systems performing development must be IA compliant, the use of compilers and other development tools on these systems are permitted with approval from the organization's Authorizing Official.

Testing and evaluation will be on IA-compliant systems to ensure compatibility with DoD live operational networks prior to migration.

3.2 Zone B Environment

Zone B follows and is similar to Zone A from a network connectivity perspective, but with much stricter control mechanisms in the infrastructure supporting the environment.

The Zone B environment is the designated zone permitting connectivity for moving sanitized data for testing purposes along with development of applications destined for a live and operational DoD network. The environment will have an IA-compliant infrastructure where it is separated from other test and development zones through the use of a firewall. Network segmentation is important in the environment because there will be areas where development and testing of products will take place with systems that will not be IA compliant. Network segments where development systems need access to tools or information outside of the environment will need to transit through a test and development DMZ for both inbound and outbound traffic. Network segments with systems that are not IA compliant will have all traffic

blocked at the T&D DMZ. Non-compliant designated network segments within the environment will not have access to any systems on network segments or other designated segments used in development since the network segments will have access to the DISN through the T&D DMZ.

Access to the Zone B environment will require an encrypted connection that will commensurate with the level of sensitivity of the network. The VPN used for access into the zone must terminate prior to access to the environment. All traffic will be inspected after VPN termination for traffic between the remote endpoint. This connectivity is to permit connectivity to network segments designated for development or testing where IA-compliant machines reside. The end user will access these network segments through a virtual guest, from a non-DoD operational network segment. When the VPN is connected, the VPN policy pushed to the client will prohibit split tunneling and will follow proper DoD policy and IA requirements for secure remote computing. The organization must prohibit direct access into non-IA compliant network segments within Zone B unless the infrastructure is configured to use a remote terminal solution to proxy access to those segments while using the VPN connection. Some examples of access into the environment are thin clients, terminal services, Citrix, and VMware solutions.

Full development within the environment will be crucial for initial coding and tweaking of products in development phase. While systems performing development must be IA compliant, permitting the use of compilers and other documented development tools on these systems is permissible.

Testing and evaluation within the environment includes non-persistent systems with limited activity and connectivity on the network. Since these systems will typically be non-IA-compliant, logical or physical separation is acceptable to keep systems from accessing any development areas within the environment. Products, applications, or other systems tested in these environments will have prohibitive access controls to DoD operational networks.

3.3 Zone C Environment

Zone C environments are specific in nature to organization's that have a mission to interconnect with other organization's to create a fully closed multi-environment network for product testing and evaluation. Because the Zone C environment will involve multiple organizations' interconnecting with one another in a Community of Interest (COI), keeping proper documentation is required. Memorandums of Understandings, Memorandums of Agreements, or other contracts must be in place and agreed upon by all of the Authorizing Officials whose organization is connecting to another organization directly or a COI.

In Zone C, the network will be isolated from the rest of an organization's operational network. Direct access to the DISN is not permitted for Zone C environments as the DISN is used to transmit data between environments. Technologies used to transit tunneled data across the DISN may be IPSec VPNs, TACLANEs, GRE tunnels, and MPLS. Please note the previously listed technologies are the most common methods of moving data been environments in a designated COI; however, it is not an inclusive list as other tunneling mechanisms may be used. As data transits the DISN through tunneling mechanisms, there must be assurance the

information sent and received is not intercepted for confidentiality purposes or manipulated in anyway compromising integrity. All traffic transiting through tunnels must be encrypted to the highest standard required for the sensitivity of data being sent and received. Unclassified traffic will employ the use of FIPS 140-2 validated cryptographic modules and classified traffic will use NSA-approved encryption. The network infrastructure supporting these connections along with the supporting infrastructure will remain IA compliant per DoD policy and IA requirements to ensure risk is kept to an acceptable level.

The organization must prohibit access from external networks outside of the trusted COI at all times.

Security requirements of systems being tested and evaluated are at the discretion of the ISSM. The ISSM will assess if testing requires systems needs to be IA compliant. If the ISSM determines systems need to be IA compliant then the systems will be loaded into an asset management system, and security requirements met.

3.4 Zone D Environment

The Zone D environment is a fully closed and physically separate network from any DoD live operational network. Permitted activities in the environment includes, but are not limited to, extensive testing using prohibited tools, working with malicious code, virus samples, working with Ports, Protocols, and Services (PPS) that are otherwise restricted via DoD policy. If the environment does not intend to include any development nor any Internet access, then all requirements are at the discretion of the ISSM.

This environment will be fully closed and isolated to any outside traffic. In the case that an Internet Service Provider (ISP) is requested for outside connectivity for research, an ISP Global Information Grid (GIG) waiver must be granted and kept current. For any Zone D environment connected to the Internet, the perimeter devices protecting the environment must remain IA compliant. If any development occurs within the environment, then the development systems must either be restricted from Internet access or at minimum, logically separated from the rest of the Zone D environment. Access Control Lists (ACLs) must be in place so inbound traffic into the development network segment is blocked.

Remote access from any DoD network/platform is prohibited. Any other remote access to the environment must ensure IA-compliance through the use of applicable security guides, such as the Secure Remote Computing, Network Infrastructure Policy, and device specific STIGs or SRGs.

Development within the environment is generally not an encouraged practice. If development occurs, all systems performing development must be IA compliant. The use of compilers and other development tools on these systems will be permitted with documented approval from the organization's AO. Prohibiting the connection of development systems within the environment connected to any internal network configured for the environment is required, in particular if Internet access is available. Any applications developed in the environment must be in compliance with the Application Security and Development (ASD) STIG. All applications must

go through a code review to ensure the application will not pose a risk to DoD networks when migrated.

Any Zone D requirements where there is not application development or Internet Access will be at the full discretion of the organization's ISSM. Since the Zone D environment is a high-risk area, any development occurring in the environment where an ISP is connected will result in the use and applicability of the Zone B STIG requirements.

Table 3-1: Environment (Zone) Applicability Table

Environment	STIG Compliancy	Remote Access	DMZ Required
Zone A Environment	Yes	Yes	Yes
Zone B Environment	ISSM discretion, with IA-compliant gateway if connected to a DoD operational network.	Yes, via non-production VLAN and non-production client if accessing non-IA-compliant systems in the environment.	Yes
Zone C Environment	ISSM discretion	No, except from alternate test site.	No
Zone D Environment	ISSM discretion	Yes, only allowed from non-production T&D client workstations and systems, if required.	No
Network Infrastructure Supporting Environments	Yes	Yes, where applicable security requirements are met.	Yes, where applicable security requirements are met.

4. VIRTUALIZATION

While implementing virtualized systems into T&D environments to reduce infrastructure costs, security should be a priority to thwart the risk of data theft or other malicious attacks and unintentional activity in the virtualized environment. Virtualizing the T&D environment can be a great way to reduce overall systems and save time in standing up new testing platforms in an ever-growing environment. However, relaxing separation restrictions should be assessed when dealing with different levels of data sensitivity and classification. The most important rule is that no system spanning classifications levels shall be allowed to reside on the same physical host. Securing systems to the highest classification otherwise is necessary, the risk for potential theft and spillage may occur.

Virtualization within differing zones may occur but only if they reside with other like systems. Secure virtualized development systems may not reside on the same physical platform or share the same hypervisor as a non-compliant virtualized testing platform. Zone A and B may be shared across physical hosts if the systems are separated in a systematic manner where proper logical separation is configured and IA-compliant T&D standards are met. All physical hosts running the hypervisor must be IA compliant when connected to any network with outside connectivity. They must be managed through a network segment dedicated for management work only.