

SITE DETAIL REPORT

CONTROL SYSTEMS CYBERSECURITY EVALUATION



CYBER SECURITY EVALUATION TOOL

CSET

CSET Viability Test 03

10/4/2018

Assessor:



Homeland Security

Disclaimer

The analysis, data, and reports in CSET® are provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

DHS does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia, or other visual identities of DHS. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office.

Advisory

CSET® is only one component of the overall cybersecurity picture and should be complemented with a robust cybersecurity program within the organization. A self-assessment with CSET cannot reveal all types of security weaknesses, and should not be the sole means of determining an organization's security posture.

The tool will not provide a detailed architectural analysis of the network or a detailed network hardware/software configuration review. It is not a risk analysis tool so it will not generate a complex risk assessment. CSET is not intended as a substitute for in depth analysis of control system vulnerabilities as performed by trained professionals. Periodic onsite reviews and inspections must still be conducted using a holistic approach including facility walk downs, interviews, and observation and examination of facility practices. Consideration should also be given to additional steps including scanning, penetration testing, and exercises on surrogate, training, or non-production systems, or systems where failures, unexpected faults, or other unexpected results will not compromise production or safety.

CSET assessments cannot be completed effectively by any one individual. A cross-functional team consisting of representatives from operational, maintenance, information technology, business, and security areas is essential. The representatives must be subject matter experts with significant expertise in their respective areas. No one individual has the span of responsibility or knowledge to effectively answer all the questions.

Data and reports generated by the tool should be managed securely and marked, stored, and distributed in a manner appropriate to their sensitivity.

TABLE OF CONTENTS

Table Of Contents.....4

Alternate Justification Comments.....5

Component Question Details:.....21

ALTERNATE JUSTIFICATION COMMENTS

Access Control #1		
Question:	Does the information system prevent and audit the execution of privileged functions by non-privileged users?	Alternate
Alternate Justification:	Gaps: Endpoint assignees are local admin. No centralized means to audit execution of privileged function. Addressed by: POAM item AC1	

Access Control #2		
Question:	Are user sessions terminated automatically based upon defined conditions (e.g. 15 minute timeouts)?	Alternate
Alternate Justification:	Gaps: UI sessions not auto-terminated Addressed by: POAM item AC2	

Access Control #3		
Question:	Does the organization encrypt controlled unclassified information on mobile devices?	Alternate
Alternate Justification:	Gaps: BYOD mobile device mail clients enrollment does not require encrypted storage. Addresses by: POAM item AC3	

Access Control #4		
Question:	Does the organization restrict access to privileged functions and security information to authorized personnel?	Alternate
Alternate Justification:	Gaps: End user regular user accounts are privileged on their endpoints. Addresses by: POAM item AC1	

Access Control #5		
Question:	Are access control policies and associated access mechanisms to control access to the system?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard)	

	Addressed by: POAM item AC5
--	--------------------------------

Access Control #9		
Question:	Does the system: (a) display the system use information before granting further access; (b) ensure that any references to monitoring, recording, or auditing are consistent with privacy accommodations for such systems that generally prohibit those activities; and (c) include a description of the authorized uses of the system?	Alternate
Alternate Justification:	Gaps: No banner message, so no references and no authorized use description. Addresses by: POAM item AC9	

Access Control #11		
Question:	Is multifactor authentication used for local access to non-privileged accounts?	Alternate
Alternate Justification:	Gaps: No MFA implemented for any use case. Addresses by: POAM item AC11	

Account Management #1		
Question:	Are user account names different than email user accounts?	Alternate
Alternate Justification:	Gaps: External email address same as UPN and email address contains samaccountname. Addresses by: POAM item AM1	

Account Management #2		
Question:	Are user or device identifiers disabled after a time period of inactivity (e.g., 30 days)?	Alternate
Alternate Justification:	Gap: Identifiers (user and computer) are not disabled stemming from lapsed activity. Addresses by: POAM item AM2	

Account Management #3		
Question:	Are users of system accounts with access to a defined list of security functions or security-relevant information required to use non-privileged accounts when accessing other system functions?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard)	

	Addressed by: POAM item AM3
--	--------------------------------

Account Management #7		
Question:	Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) Addressed by: POAM item AM7	

Audit and Accountability #1		
Question:	Are alerts responded to in a timely manner?	Alternate
Alternate Justification:	Gaps: Alert response times and SLAs not fully developed. Addressed by: POAM item AA1	

Audit and Accountability #2		
Question:	Is there a real-time alert when any defined event occurs?	Alternate
Alternate Justification:	Gaps: Incomplete audit capturing capability. No solution to detect/notify if existing audit capturing systems have failed (due to storage/hardware failures, etc.). Addressed by: POAM item AA2 Notes: 3.3.4 is focused on lack of alert due to an undetected fault/failure in the audit capturing system.	

Audit and Accountability #3		
Question:	Does the system provide an audit reduction and report generation capability?	Alternate
Alternate Justification:	Gaps: Incomplete audit capturing and reduction capability Addressed by: POAM item AA2	

Audit and Accountability #4		
Question:	Are automated mechanisms used to integrate audit review, analysis, and reporting into processes for investigation and response to suspicious activities?	Alternate
Alternate Justification:	Gaps: Incomplete audit capturing capability.	

	Addressed by: POAM item AA2 Notes: 3.3.1 is focused on the creation, protection, and retention of audit records as a basic requirement.
--	--

Audit and Accountability #5		
Question:	Are the permitted actions specified for each authorized information system process, role, and/or user in the audit and accountability policy?	Alternate
Alternate Justification:	Gaps: Role based access not consistently or rigorously applied across enterprise and not stipulated in Doc hierarchy. Addressed by: POAM item AA5	

Audit and Accountability #6		
Question:	Is there the capability to automatically process audit records for events of interest based on selectable event criteria?	Alternate
Alternate Justification:	Gaps: Audit reduction capability limited to a couple systems. No enterprise-level capability. Addressed by: POAM item AA2	

Audit and Accountability #7		
Question:	Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?	Alternate
Alternate Justification:	Gaps: No SIEM solution to capture audit information, so no audit information to protect. Addressed by: POAM item AA2	

Audit and Accountability #8		
Question:	Is the list of defined auditable events reviewed and updated on a defined frequency?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating identifying and periodically reviewing auditable events Addressed by: POAM item AA8	

Audit and Accountability #9		
Question:	Does the system protect against an individual falsely denying having performed a particular action?	Alternate
Alternate Justification:		

	<p>Gaps: Logging configuration for datastores and applications housing sensitive data not uniformly configured to capture who did what when.</p> <p>Addressed by: POAM item AA9</p>
--	---

Audit and Accountability #10		
Question:	Is access to management of audit functionality authorized only to a limited subset of privileged users? Are audit records of nonlocal accesses to privileged accounts and the execution of privileged functions protected?	Alternate
Alternate Justification:	<p>Gaps: Audit functionality management not restricted on endpoints because each employee is local admin on his/her endpoint. Otherwise it is appropriately restricted.</p> <p>Addressed by: POAM item AA10</p>	

Communication Protection #1		
Question:	Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?	Alternate
Alternate Justification:	<p>Gaps: Though robust technological solutions are in place at both external and key internal boundaries, there are numerous cases where their configuration must be more stringent to meet our control objectives. Likewise we need to improve and integrate the monitoring of these solutions.</p> <p>Addressed by: POAM item CP1</p> <p>Notes: 3.13.5 is addressed by the current DMZ deployment</p>	

Communication Protection #2		
Question:	Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?	Alternate
Alternate Justification:	<p>Gaps: At some branch offices firewalls are currently configured such that they would not interdict an unauthorized alternative gateway connection from an on-site device.</p> <p>Addressed by: POAM item CP2</p>	

Communication Protection #3		
Question:	Does the system deny network traffic by default and allow network traffic by exception?	Alternate
Alternate Justification:	<p>Gaps: As noted in CP2, at some branch offices firewalls are currently configured such that they would not interdict an unauthorized alternative gateway connection from an on-site device.</p> <p>Addressed by: POAM item CP2</p>	

Communication Protection #4		
Question:	Does the system prevent remote devices that have established connections (e.g., PLC, remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?	Alternate
Alternate Justification:	<p>Gaps: Though an in-flight project is currently correcting this, split tunnelling is currently enabled for some endpoint devices.</p> <p>Addressed by: POAM item CP4</p>	

Communication Protection #8		
Question:	Does the organization document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?	Alternate
Alternate Justification:	<p>Gaps: We have not currently deployed or enabled a solution that could detect and interdict unauthorized flows of CUI. We have not established a classification standard (which would include CUI as a type) and other document hierarchy elements to drive use of data classification. We have not indoctrinated the workforce in data classification standards and their usage.</p> <p>Addressed by: POAM item CP8</p> <p>Note: 3.1.3 and AC-4 are specifically about controlling where CUI is allowed to travel, distinct from who is allowed to access it.</p>	

Configuration Management #1		
Question:	Are individual access privileges, physical access, and logical access restrictions associated with configuration changes to the system defined, documented, and approved?	Alternate
Alternate Justification:	<p>Gaps: Though our physical and logical access controls generally restrict ability to change configuration to people in the correct roles, we lack the policy, control objective, and standard documentation hierarchy components that our change management program should be based on. These guiding components will require refinements to the existing change request workflow.</p> <p>Addressed by: POAM item CM2</p> <p>Notes: This item is focused defining and enforcing access restrictions -- administrative and technological -- that constrain the access to make changes to the system to only those explicitly allowed to, and further to specific tasks at planned times stemming from review and approval.</p>	

Configuration Management #5		
Question:	Are configuration changes tested, validated, and documented before installing them on the operational system, and has testing been ensured to not interfere with system operations?	Alternate
Alternate Justification:	<p>Gaps: Pre-approval testing, validation, and documentation, as well as preventing testing from disrupting production operations are not an explicitly required part of the change management process.</p>	

	Addressed by: POAM item CM5
--	--------------------------------

Configuration Management #6		
Question:	Are mandatory configuration settings used for products employed within the system?	Alternate
Alternate Justification:	Gaps: Baseline security configuration settings for system devices are not consistently defined or validated before deployment, nor do documentation hierarchy elements exist to require that. Addressed by: POAM item CM6	

Configuration Management #7		
Question:	Is there a defined list of software programs authorized to execute on the system? Is the authorization policy a deny-all, permit-by-exception for software allowed to execute on the system? Is it reviewed at least annually?	Alternate
Alternate Justification:	Gaps: Software program execution is not currently managed or controlled. Addressed by: POAM item AC1	

Continuity #1		
Question:	Does the alternate processing site provide information security measures equivalent to that of the primary site?	Alternate
Alternate Justification:	Gaps: When endpoint is off prem it lacks next-gen firewall protections. Addressed by: POAM item C1	

Incident Response #2		
Question:	Does the organization test its incident response capabilities?	Alternate
Alternate Justification:	Gaps: There is no standard requiring incident response plan testing, nor is periodic testing currently performed. Addressed by: POAM item IR2	

Incident Response #4		
Question:	Are personnel required to report suspected security incidents to the organizational incident response authority within a defined time-period?	Alternate
Alternate Justification:		

	<p>Gaps: IR-related documentation hierarchy elements are incomplete. There is currently no explicitly-stated requirement for staff to report suspected security incidents and in what time frame.</p> <p>Addressed by: POAM item IR4</p>
--	--

Information Protection #1		
Question:	Is removable system media and system output marked indicating the distribution limitations, handling caveats, and applicable security markings?	Alternate
Alternate Justification:	<p>Gaps: Data classification system and related media marking standards, including for CUI, do not exist yet.</p> <p>Addressed by: POAM item IP1</p>	

Information Protection #2		
Question:	Is system digital and non-digital media sanitized before disposal or release for reuse?	Alternate
Alternate Justification:	<p>Gaps: Data classification system and related sanitization requirements, including for CUI, do not exist yet.</p> <p>Addressed by: POAM item IP2</p>	

Information Protection #3		
Question:	Is the system media securely stored within protected areas?	Alternate
Alternate Justification:	<p>Gaps: Data classification system and related secure storage requirements, including for CUI, do not exist yet.</p> <p>Addressed by: POAM item IP3</p>	

Information Protection #4		
Question:	Is accountability for system media maintained during transport outside controlled areas?	Alternate
Alternate Justification:	<p>Gaps: Data classification system and related media transport accountability requirements including for CUI, do not exist yet.</p> <p>Addressed by: POAM item IP4</p>	

Information Protection #5		
Question:	Are cryptographic mechanisms used to protect digital media during transport outside of controlled areas?	Alternate
Alternate Justification:	<p>Gaps: Data classification system and related encryption requirements for transport, including for CUI, do not exist yet.</p>	

	Addressed by: POAM item IP5
--	--------------------------------

Maintenance #4		
Question:	Is the use of system maintenance tools approved and monitored?	Alternate
Alternate Justification:	Gaps: Documentation hierarchy stipulating the the requirement and standards for tools, mechanisms, and personnel to be approved and monitored is lacking. Addressed by: POAM item MT4	

Maintenance #6		
Question:	Does the system require multifactor authentication for remote maintenance access?	Alternate
Alternate Justification:	Gaps: Two factor authentication is currently only employed for a pilot group. Addressed by: POAM items AC2	

Maintenance #7		
Question:	Are all sessions and remote connections terminated when remote maintenance is completed?	Alternate
Alternate Justification:	Gaps: Session autotermination is not currently implemented. Addressed by: POAM items AC11	

Media Protection #1		
Question:	Does the organization limit CUI media access to authorized users?	Alternate
Alternate Justification:	Gaps: Data classification system and related least privilege requirements, including for CUI, do not exist yet. Addressed by: POAM item MP1	

Monitoring & Malware #4		
Question:	Is unauthorized use of the system identified? (e.g., log monitoring)	Alternate
Alternate Justification:	Gaps: No SIEM solution to capture and consolidate system use, so tracking of unauthorized use is fragmented and incomplete. Addressed by:	

	POAM item AC1
--	---------------

Monitoring & Malware #6		
Question:	Is there an organizational policy defining the frequency of vulnerability scans?	Alternate
Alternate Justification:	Gaps: The org recently procured an enterprise vulnerability and baseline scanning system but has yet to begin deployment. Addressed by: POAM item MM6	

Monitoring & Malware #7		
Question:	Is the list of system vulnerabilities scanned updated on a defined frequency or when new vulnerabilities are identified and reported?	Alternate
Alternate Justification:	Gaps: The org recently procured an enterprise vulnerability and baseline scanning system but has yet to begin deployment. Addressed by: POAM item MM6	

Personnel #2		
Question:	Are electronic and physical access permissions reviewed when individuals are reassigned or transferred?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating review of electronic and physical access permissions during and after personnel actions such as terminations and transfers. Addressed by: POAM item PT1	

Physical Security #1		
Question:	Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?	Alternate
Alternate Justification:	Gaps: Physical access control patterns and practices are not uniform across the enterprise. There is a lack of document hierarchy elements (policy, control objective, standard) stipulating the requirements for physical access controls. Addressed by: POAM item PS1 Notes: This item is specifically focused on physical access control to BC systems.	

Physical Security #2		
Question:	Is physical access monitored to detect and respond to physical security incidents?	Alternate

Alternate Justification:	<p>Gaps: Physical access control patterns and practices are not uniform across the enterprise. There is a lack of document hierarchy elements (policy, control objective, standard) stipulating the requirements for physical access monitoring.</p> <p>Addressed by: POAM item PS2</p>
--------------------------	---

Physical Security #4		
Question:	Are visitors escorted and monitored as required in the security policies and procedures?	Alternate
Alternate Justification:	<p>Gaps: Physical access control patterns and practices are not uniform across the enterprise. There is a lack of document hierarchy elements (policy, control objective, standard) stipulating the requirements for escorting and monitoring of visitors.</p> <p>Addressed by: POAM item PS1</p>	

Physical Security #5		
Question:	Are visitor access records maintained, and are all physical access logs retained for as long as required by regulations or per approved policy?	Alternate
Alternate Justification:	<p>Gaps: Physical access control patterns and practices are not uniform across the enterprise. There is a lack of document hierarchy elements (policy, control objective, standard) stipulating the requirements for visitor access records and physical access logs retention.</p> <p>Addressed by: POAM item PS5</p>	

Plans #3		
Question:	Is the risk assessment plan updated annually or whenever significant changes occur to the system, the facilities where the system resides, or other conditions that may affect the security or accreditation status of the system?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating the digital services risk management model, including requirements for periodic and as-needed re-assessment.</p> <p>Addressed by: POAM item RM3</p>	

Policies & Procedures General #1		
Question:	Is the system managed using a system development life-cycle methodology that includes security considerations?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) defining system development lifecycle requirements and practices, including baseline configurations and system inventories that address security.</p> <p>Addressed by: POAM item PPG1</p>	

Portable/Mobile/Wireless #1		
Question:	Is the use of mobile code documented, monitored, and managed? (Java, JavaScript, ActiveX, Postscript, etc.)	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating documentation, monitoring and management requirements for mobile code, so such controls are at best partial.</p> <p>Addressed by: POAM item PMW1</p>	

Portable/Mobile/Wireless #2		
Question:	Is each mobile device connection to the system authorized?	Alternate
Alternate Justification:	<p>Gaps: Lack of an official request and authorization process for mobile device connections.</p> <p>Addressed by: POAM item PMW2</p>	

Portable/Mobile/Wireless #4		
Question:	Is the use of writable, removable media restricted on the system?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating acceptable use and control requirements for removable media. Technological controls not configured to restrict and control removable media use.</p> <p>Addressed by: POAM item PMW4</p>	

Remote Access Control #1		
Question:	Are restrictions imposed on authorized individuals with regard to the use of organization-controlled removable media on external systems?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating acceptable use and control requirements for removable media, including restrictions pertaining to connection to external information systems. Technological controls not configured to restrict and control removable media use.</p> <p>Addressed by: POAM item RAC1</p>	

Remote Access Control #2		
Question:	Are all the methods of remote access to the system authorized, monitored, and managed?	Alternate
Alternate Justification:	<p>Gaps: Remote access session monitoring is partial at best.</p> <p>Addressed by: RAC2</p>	

Remote Access Control #5		
Question:	Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) defining that remote execution of privileged commands and remote access to security-relevant info is subject to authorization and defining the rationale for such access to systems.</p> <p>Addressed by: POAM item RAC5</p>	

Risk Management and Assessment #1		
Question:	Is there an independent assessor or assessment team to monitor the security controls in the system on an ongoing basis?	Alternate
Alternate Justification:	<p>Gaps: Control requirements are only now being defined at the security program level and security controls are not monitored on an ongoing basis to measure/validate their effectiveness.</p> <p>Addressed by: POAM item RMA1</p>	

Risk Management and Assessment #2		
Question:	Are the security controls in the system assessed on a defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome?	Alternate
Alternate Justification:	<p>Gaps: Control requirements are only now being defined at the security program level, including identifying the desired outcomes that provide the basis for those control requirements, and the need to reassess the security control system at least annually.</p> <p>Addressed by: POAM item RMA2</p>	

System and Communications Protection #1		
Question:	Are systems configured to prohibit remote activation of collaborative computing (e.g., IM, video conferencing) and is there an indication of use to the local user?	Alternate
Alternate Justification:	<p>Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating prohibition of remote activation of collaborative computing systems, including requiring indicator to users present that the device is activated. Lack of corresponding baseline configuration requirement.</p> <p>Addressed by: POAM item SCP1</p>	

System and Services Acquisition #1		
Question:	Are system security engineering principles applied in the specification, design,	Alternate

	development, and implementation of the system?	
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating architectural standards, software development practices, and systems engineering principles to promote effective security in the organization's information systems. Addressed by: POAM item: SSA1	

System Integrity #1		
Question:	Are system flaws identified, reported, and corrected?	Alternate
Alternate Justification:	Gaps: Only a partial scope of system types have system flaw detection, reporting, and remediation. Addressed by: POAM item SI1	

System Integrity #2		
Question:	Is the time between flaw identification and flaw remediation measured and compared with benchmarks?	Alternate
Alternate Justification:	Gaps: Only a partial scope of system types have system flaw detection, reporting, and remediation, and there is not yet a formal metric for the timeframe in which flaws must be corrected. Addressed by: POAM item SI2	

System Integrity #3		
Question:	Are internal security alerts, advisories, and directives generated?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) requiring monitoring information system security alerts and advisories, disseminating them internally, and taking appropriate actions in response. Addressed by: POAM item SI3	

System Integrity #5		
Question:	Have unused removable media support files been removed or disabled?	Alternate
Alternate Justification:	Gaps: Lack of document hierarchy elements (policy, control objective, standard) stipulating marking removable to indicate the owner and prohibiting use of such media that lacks owner identification. Addressed by: POAM item SI5	

System Protection #2		
Question:	Does the system protect the confidentiality of information at rest? (e.g., disk encryption)	Alternate
Alternate Justification:	Gaps: At-rest data encryption capability is incomplete and is not explicitly required or provided for in cases where CUI may be stored. Addressed by: POAM item SP2	

System Protection #3		
Question:	Is the system configured to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in a "prohibited and/or restricted" list?	Alternate
Alternate Justification:	Gaps: Systems are not consistently checked to be sure only required services and functions are enabled prior to system release. Likewise, document hierarchy elements (policy, control objective, standard) stipulating this release requirement are not yet in place. Addressed by POAM item SP3	

System Protection #4		
Question:	Are automated mechanisms used to prevent program execution in accordance with defined lists? (e.g., white listing)	Alternate
Alternate Justification:	Gaps: Software program execution is not currently managed or controlled. Addressed by: POAM item AC1	

System Protection #5		
Question:	Does the system employ processing components that have minimal functionality and data storage (e.g., diskless nodes, thin client technologies)?	Alternate
Alternate Justification:	Gaps: Use cases for which thin nodes would be sufficient and recommended are not defined or established. Addressed by: POAM item SP5	

Training #1		
Question:	Is basic security awareness training provided to all system users before authorizing access to the system, when required by system changes and at least annually thereafter?	Alternate
Alternate Justification:	Gaps: Security awareness training for system users -- initial, recurring, or otherwise -- is not implemented. Addressed by: POAM item TRAIN1	

Training #2		
Question:	Are practical exercises included in the security awareness training that simulate actual cyber-attacks?	Alternate
Alternate Justification:	Gaps: Security awareness training for system users -- initial, recurring, or otherwise -- is not implemented, so simulated attacks are not either. Addressed by: POAM item TRAIN2	

Training #3		
Question:	Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on an periodic basis?	Alternate
Alternate Justification:	Gaps: Security awareness training for system users -- initial, recurring, or otherwise -- is not implemented. Addressed by: POAM item TRAIN1	

COMPONENT QUESTION DETAILS:

Component:			
Question:			
Zone:		SAL:	