Risk Management Assessment

FY19
Q4/Anual
Modified

Office of Government Ethics

Overall Summary

Function	Security Domain	Rating	Agency Comments
Identify		Managing Risk	
	Asset Management	Managing Risk	
	System Authorization	Managing Risk	
Protect		Managing Risk	
	Remote Access Protection	Managing Risk	
	Credentialing and Authorization	At Risk	
	Configuration and Vulnerability Management	At Risk	
	HVA Protection	Managing Risk	
Detect		Managing Risk	
	Intrusion Detection and Prevention	Managing Risk	
	Exfiltration and Enhanced Defenses	Managing Risk	
Respond and Recover		At Risk	
	Respond and Recover	At Risk	
Overall		**Managing Risk**	

Identify

Security Domain: Asset Management

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Automated hardware asset management: GFE hardware assets are covered by an automatic hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level [1.2.4 / (1.2.1 + 1.2.2 + 1.2.3) >= 95%]	100%	95%	Managing Risk	85	Agree	
Automated software asset management: GFE endpoints are covered by an automated software asset inventory capability at the enterprise-level [1.2.5 / 1.2.1 >= 95%]	100%	95%	Managing Risk	84	Agree	
Unauthorized hardware alerts: Unclassified network has implemented a technology solution centrally visible at the enterprise-level to detect and alert on the connection of unauthorized hardware assets. [3.9 >= 95%]	100%	95%	Managing Risk	81	Agree	
Unauthorized software alerts: Number of GFE endpoints (from 1.2.1.) covered by a software asset management capability centrally visible at the enterprise-level that is able to block or prevent unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions). [3.10.1 / 1.2.1 >= 95%]	100%	95%	Managing Risk	74	Agree	
Remote mobile device wiping: Mobile assets operate under an enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices. [(1.3.3 + 1.3.4) / (1.3.1 + 1.3.2) >= 95%]	100%	95%	Managing Risk	94	Agree	

Security Domain: System Authorization

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments

Identify

Security Domain: System Authorization

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
High Impact Systems have ATOs: High impact systems operate with a security Authority to Operate (ATO). [High 1.1.3 / (1.1.1 + 1.1.2) = 100%]	N/A	100%	Not Applicable	85	Agree	
Moderate Impact Systems have ATOs: Moderate impact systems operate with a security Authority to Operate (ATO). [Moderate 1.1.3 / (1.1.1 + 1.1.2) = 100%]	100%	100%	Managing Risk	93	Agree	

Protect

Security Domain: Remote Access Protection

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Encrypted Remote Connections. Remote access connections utilize FIPS 140-2 validated cryptographic modules. [(Lower of 2.10.1) = 100%]	100%	100%	Managing Risk	88	Agree	
Remote connections timeout after 30 minutes. Remote access connections time out after 30 minutes (or less) of inactivity and requires re-authentication to re-establish a session. [(Lower of 2.10.2) = 100%]	100%	100%	Managing Risk	85	Agree	
Prohibit dual remote connections. Remote access connections prohibit the use of split tunneling and/or dual-connected remote hosts where the connecting device has two active connections. [Lower of 2.10.3] = 100%	100%	100%	Managing Risk	84	Agree	

Security Domain: Credentialing and Authorization

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Unprivileged users required to log on with IAL/AAL 3. Unprivileged users are required to authenticate to the network through the machine-based or user-based enforcement of a two-factor PIV credential or other Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential. [CIO 2.4.2 / 2.4.1 >= 85%]	100%	85%	Managing Risk	55	Agree	
Privileged users required to log on with IAL/AAL 3. Privileged users are required to authenticate to the network through the machine-based or user-based enforcement of a two-factor PIV credential or other Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential. [2.5.2 / 2.5.1 = 100%]	100%	100%	Managing Risk	62	Agree	

Protect

Security Domain: Credentialing and Authorization

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Local privileged accts required to log on with IAL/AAL 3. Privileged local system accounts that can access the Agency's network are required to authenticate to the network through the machine-based or user-based enforcement of a two-factor PIV credential or other Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential. [2.6.2 / 2.6.1 >= 95%]	100%	95%	Managing Risk	54	Agree	
Privileged users limited to trusted sites. Privileged users with network accounts that have a technical control limiting access to only trusted sites. [2.3 >= 90%]	0%	90%	High Risk	73	Agree	
Unprivileged centralized access management. Unprivileged users are covered by a centralized dynamic access management solution that controls and monitors users access. [2.4.4 / 2.4.1 >= 95%]	100%	95%	Managing Risk	70	Agree	
Privileged centralized management. Privileged users are covered by a centralized dynamic access management solution that controls and monitors users' access. [2.5.4 / 2.5.1 >= 100%]	100%	100%	Managing Risk	72	Agree	

Security Domain: Configuration and Vulnerability Management

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Systems assessed by SCAP products. Devices on the network assessed for vulnerabilities by a solution centrally visible at the enterprise-level that is Security Content Automation Protocol (SCAP) validated or uses National Vulnerability Database (NVD) information. [2.1 / (1.2.1 + 1.2.2 + 1.2.3)]>=95%	100%	95%	Managing Risk	85	Agree	
Assets comply with security configuration baseline. GFE hardware assets covered by auditing for compliance with common security configuration baseline. [2.2.3 / 2.2.1 >= 95%]	100%	95%	Managing Risk	94	Agree	

Protect

Security Domain: Configuration and Vulnerability Management

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
HVA automated flaw remediation solution. HVA systems are covered by an automated mechanism to determine the state of information system components with regard to flaw remediation (i.e., software patching). [2.13 / (Number of HVAs)] >= 90%	100%	90%	Managing Risk	84	Agree	
HVA central flaw remediation solution. HVA systems are covered by a central, enterprise-level automated mechanism to determine the state of information system components with regard to flaw remediation (i.e., software patching). [(2.13.1 / 2.13)] >= 90%, if 2.13 is 0 this capability is considered "High Risk"	0%	90%	High Risk	86	Agree	
Automated removable media prevention. GFE endpoints are covered by an automated mechanism to prevent the usage of untrusted removable media. [(2.12 / 1.2.1) >= 90%]	100%	90%	Managing Risk	54	Agree	

Security Domain: HVA Protection

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
HVAs encrypt data at rest. HVA systems encrypt all Federal Information at rest. [2.8 / (Number of HVAs - 2.8.1)]>=90%	100%	90%	Managing Risk	59	Agree	
HVAs require IAL/AAL 3 authentication. HVA systems require all government and contractor users (100% privileged and unprivileged) to authenticate through the machine-based or user based enforcement of a two-factor PIV credential or other IAL3/AAL3 credential. [2.7 / (Number of HVAs - 2.7.1) >= 90%]	100%	90%	Managing Risk	53	Agree	
HVAs are logically segmented. HVA systems' networks are segmented from other accessible systems and applications in the agency's network(s). [2.9 / (Number of HVAs - 2.9.1) >= 90%]	100%	90%	Managing Risk	60	Agree	

Detect

Security Domain: Intrusion Detection and Prevention

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
DMARC set to default 'reject': Email traffic analyzed using Domain-based Message Authentication, Reporting & Conformance (DMARC) email authentication protocols, set to a policy of 'reject' on all second-level .gov and mail-sending hosts. BOD 18-01 report indicates 100% 'reject' on all second-level .gov and mail-sending hosts	100%	100%	Managing Risk	74	Agree	
Emails analyzed for malicious attachments: Incoming email traffic analyzed for suspicious or potentially malicious attachments without signatures that can be tested in a sandboxed environment or detonation chamber. [3.2 >= 90%]	100%	90%	Managing Risk	90	Agree	
Intrusion prevention systems coverage: GFE endpoints are covered by an intrusion prevention system, where actions taken by the system are centrally visible at the enterprise-level. [3.3 / 1.2.1 >= 90%]	100%	90%	Managing Risk	95	Agree	
Antivirus coverage: GFE endpoints are covered by an antivirus (AV) solution that provides file reputation services that check suspicious files against continuously updated malware information in near real-time. [(3.4 / 1.2.1) >= 90%]	100%	90%	Managing Risk	98	Agree	
Anti-exploitation tool coverage: GFE endpoints are covered by a capability that protects memory from unauthorized code execution (e.g., Data Exploitation Prevention (DEP), Address Space Layout Randomization (ASLR)). [(3.5 / 1.2.1) >= 90%]	100%	90%	Managing Risk	86	Agree	
Browser tool blocking phishing websites and IPs: GFE endpoints are protected by a browser-based or enterprise-based tool to block known phishing websites and IP addresses. [3.6 / 1.2.1 >= 90%]	100%	90%	Managing Risk	92	Agree	
Assets scanned for malware before connecting: Assets are scanned for malware prior to an authorized remote access connection to the unclassified network. [3.7 / 2.11 >= 90%]	91%	90%	Managing Risk	68	Agree	

Detect

Security Domain: Exfiltration and Enhanced Defenses

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
Outbound traffic checked for unauthorized exfiltration: Outbound communications traffic is checked at the external boundaries to detect potential unauthorized exfiltration of information (e.g. anomalous volumes of data, anomalous traffic patterns, elements of PII, etc.) with a solution that is centrally visible at the enterprise-level. [3.8 >= 90%]	100%	90%	Managing Risk	82	Agree	
EINSTEIN capabilities implemented: Network is protected by E1/E2, E3A DNS Sinkholing, and E3A Email Filtering capabilities [EINSTEIN onboarding report indicates 'Complete' for all capabilities] [External Data Administration Count = 3]	3	3	Managing Risk	2	Agree	

Respond and Recover

Security Domain: Respond and Recover

Capability	Value	Target	Rating	Gov. Wide	Agency Response	Agency Comments
No active critical vulnerabilities: Critical vulnerabilities, based on an industry-standard scoring model, are remediated as quickly as possible. BOD 19-02 reporting indicates no 15+ day critical vulnerabilities	0	0	Managing Risk	0	Agree	
Automated tracking of incident information: Network covered by an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information. [4.2 = 100%]	100%	100%	Managing Risk	86	Agree	
HVAs reconfigure or disable upon security violation: HVA systems covered by a capability that can dynamically reconfigure and/or automatically disable the system or relevant asset upon the detection of a given security violation or vulnerability [4.3 / Number of HVAs >= 90%]	0%	90%	High Risk	36	Agree	
HVAs have an Information Security Contingency Plan: HVA systems have an Information System Contingency Plan (ISCP) has been developed to guide the process for assessment and recovery of the system following a disruption. [5.1 / Number of HVAs >= 90%]	100%	90%	Managing Risk	83	Agree	
HVAs have an alternate processing site: HVA systems have an alternate processing site identified and provisioned. [5.1.1 / 5.1 >= 90%]	50%	90%	High Risk	77	Agree	