Information Technology (IT) System and Information Integrity (SI) Standard

January 31, 2023

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov.**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.01.30 15:22:59 -05'00'

Steven Hernandez

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Table 1: Revision History

Version	Date	Summary of Changes
1.0	1/20/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.2	1/31/2023	Annual review. Update broken links. Add footnote to HVA control reference in Section 2. Add control overlay SI-4 ED-03 to comply with OMB M-22-09.

Contents

1 INTRODUCTION

This governance document establishes Department information technology (IT) system maintenance controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these system information and integrity control standards.

2 STANDARDS

The Department standards for IT system information and integrity controls are organized to follow

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 SI-1 System and Information Integrity Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level IT system and information integrity policy (e.g., this document) that:

a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy*.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system and information integrity policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws,

[5] https://www.cisa.gov/publication/high-value-asset-control-overlay

executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated system and information integrity controls. The ISO and ISSO shall review IT system and information integrity procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 SI-2 Flaw Remediation (L, M, H and Control Overlay)

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within a timeline in accordance with Department policies and standards, the criticality of the updates, risk to the Department, prioritization of resources, and as required to comply with DHS CISA/OMB requirements for flaw remediation and patching of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Control Overlay SI-2 ED-01 (L, M, H): Install and test patches on a non-production system prior to implementation on a production system. When non-production systems are not available, the ISO in conjunction with the ISSO support must identify procedures to restore the production system in the event of patch issues.

Control Overlay SI-2 ED-02 (L, M, H): Use change management processes to approve patches prior to installation on systems.

Control Overlay SI-2 ED-03 (L, M, H): Ensure patching and remediation is implemented based on assessment of risk, prioritization of resources, and in accordance with the timelines and vulnerability criticality defined in Information Technology (IT) System Risk Assessment (RA) Standard, Appendix B: Remediation Requirements.

Control Overlay SI-2 ED-04 (L, M, H): Approve and document deviations from Department policies, instructions, standards, procedures, or memos related to patching and remediation using the Department's Risk Acceptance Form (RAF) process and an associated POA&M to track the vulnerability until it is eliminated or mitigated.

Control Overlay SI-2 ED-05 (L, M, H): Use patch management practices to maintain EO-critical software platforms and all software deployed to those platforms, including but not limited to:

a. Rapidly identify, document, and mitigate known vulnerabilities (e.g., patching, updating, upgrading software to supported version) to continuously reduce the exposure time.

b. Monitor the platforms and software to ensure the mitigations are not removed outside of change control processes.

2.2.1 SI-2(2) Flaw Remediation | Automated Flaw Remediation Status (M, H)

Determine if system components have applicable security-relevant software and firmware updates installed using ED approved automated mechanisms at least monthly.

2.3 SI-3 Malicious Code Protection (L, M, H)

a. Implement signature based and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

    1. Perform periodic scans of the system at least weekly and real-time scans of files from external sources at endpoint and network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and

    2. Block or quarantine malicious code; and send alert to the EDSOC and when feasible, to system administrators, ISO, ISSO or other personnel assigned to serve in incident response roles in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

2.4 SI-4 System Monitoring (L, M, H and Control Overlay)

a. Monitor the system to detect:

    1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: ED IT/Cybersecurity monitoring objectives as defined in ED Information Security Continuous Monitoring Roadmap; and

    2. Unauthorized local, network, and remote connections

b. Identify unauthorized use of the system through the following techniques and methods: ED approved security safeguards including but not limited to endpoint detection and response tools, continuous monitoring, vulnerability scans, malicious code protection mechanisms,

intrusion detection or prevention mechanisms, and/or boundary protection devices such as firewalls, gateways, and routers

c. Invoke internal monitoring capabilities or deploy monitoring devices:
    1. Strategically within the system to collect organization-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide ED approved information system monitoring output to the ISO and ISSO who distribute the information to DHS CISA, and other personnel with system administration, monitoring, and/or security responsibilities as needed and in accordance with Department policy.

Control Overlay SI-4 ED-01 (L, M, H): Continuously monitor the security of EO-critical software platforms and all software running on those platforms.

Control Overlay SI-4 ED-02 (L, M, H): Employ endpoint security protection on EO-critical software platforms to protect the platforms and all software running on them.

Control Overlay SI-4 ED-03 (L, M, H): Comply with OMB M-22-09 by ensuring endpoint detection and response (EDR) tools meet DHS CISA's technical requirements and are deployed widely.

2.4.1 SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis (M, H)

Employ automated tools and mechanisms to support near real-time analysis of events.

2.4.2 SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic (M, H)

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic
b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.

2.4.3 SI-4(5) System Monitoring | System-generated Alerts (M, H)

Alert personnel with incident response, system administration, monitoring, and/or security

responsibilities when the following system-generated indications of compromise or potential compromise occur:

a. ED defined list of compromised indicators or indications that the system's integrity has been breached including, but not limited to:

    1. Protected system files or directories have been modified without notification from the appropriate change/configuration management channels.
    2. System performance indicates resource consumption that is inconsistent with expected operating conditions.
    3. Auditing functionality has been disabled or modified to reduce audit visibility.
    4. Audit or log records have been deleted or modified without explanation.
    5. The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition.
    6. Resource or service requests are initiated from clients that are outside of the expected client membership set.
    7. The system reports failed logins or password changes for administrative or key service accounts.
    8. Processes and services are running that are outside of the baseline system profile.
    9. Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.

2.4.4 SI-4(10) System Monitoring | Visibility of Encrypted Communications (H)

Make provisions so that ED-approved encrypted communications traffic is visible to ED-approved system monitoring tools and mechanisms.

2.4.5 SI-4(12) System Monitoring | Automated Organization-generated Alerts (H)

Alert personnel with incident response, system administration, monitoring, and/or security responsibilities including but not limited to EDSOC and system administrators using ED-authorized automated mechanisms, including e-mail when the following indications of inappropriate or unusual activities with security or privacy implications occur: activities that trigger alerts.

2.4.6 SI-4(14) System Monitoring | Wireless Intrusion Detection (H)

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

2.4.7 SI-4(20) System Monitoring | Privileged Users (H)

Implement the following additional monitoring of privileged users: Privileged Account Management (PAM) sufficient to provide nonrepudiation for administrative actions (when technically feasible); device compliance authorization; locational account lockouts; statistical and analytical review of privileged user activity; multifactor authentication (MFA) misuse; naming policy compliance; date and time (normal operation time); and other logging requirements noted in OMB Memorandum M-21-31, dated August 27, 2021 or successor as appropriate.

2.4.8 SI-4(22) System Monitoring | Unauthorized Network Services (H)

a. Detect network services that have not been authorized or approved by ED authorization or approval processes; and

b. Audit and alert personnel with responsibilities for performing system and or network monitoring when detected.

2.5 SI-5 Security Alerts, Advisories, and Directives (L, M, H)

a. Receive system security alerts, advisories, and directives from EDSOC (e.g., ED alerts, advisories and directives as well as alerts and advisories received by ED from the CISA, OMB, etc.) as well as from external organizations, when appropriate and available, such as supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including, but not limited to Principal Offices, ISO and ISSO; and

d. Implement security directives in accordance with established timeframes or notify the issuing organization of the degree of noncompliance.

2.5.1 SI-5(1) Security Alerts, Advisories, and Directives | Automated Alerts and Advisories (H)

Broadcast security alert and advisory information throughout the organization using ED approved automated mechanisms including, but not limited to e-mail.

2.6 SI-6 Security and Privacy Function Verification (H)

a. Verify the correct operation of security and privacy functions;

b. Perform the verification of the functions specified in SI-6a on system startup, restart; and/or abort; upon command by user with appropriate privilege; every 7 days;

c. Alert designated ED personnel with information security and/or privacy responsibilities (e.g., System administrators, ISSO) to failed security and privacy verification tests; and

d. Shut down or restart the information system, and notifies system administrators, security personnel and/or privacy personnel when anomalies are discovered.

2.7 SI-7 Software, Firmware, and Information Integrity (M, H)

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: ED-authorized software, firmware, and information including, but not limited to system kernels, drivers, firmware, (e.g., BIOS) software (e.g., OS, applications, middleware) and security attributes; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify appropriate ED personnel (e.g., System Administrators).

2.7.1 SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks (M, H)

Perform an integrity check of software, firmware, and information within ED information systems: at startup or restart; at the occurrence of configuration changes or security-relevant events; the identification of a new threat to which the information system is susceptible; and installation of new hardware at least monthly.

2.7.2 SI-7(2) Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations (H)

Employ automated tools that provide notification to system administrators and other personnel with responsibilities for system/network monitoring upon discovering discrepancies during integrity verification.

2.7.3 SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations (H)

Automatically initiate ED approved incident response process when integrity violations are discovered.

2.7.4 SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response (M, H)

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: changes to established configuration settings and unauthorized elevation of system privileges.

2.7.5 2.7.5 SI-7(15) Software, Firmware, and Information Integrity | Code Authentication (H)

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: ED-approved software or firmware components.

2.8 SI-8 Spam Protection (M, H and Control Overlay)

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Control Overlay SI-8 ED-01 (L, M, H): Require all second-level agency domains to have valid SPF/DMARC records, with a policy of "reject" for second-level domains and mail-sending hosts.

2.8.1 SI-8(2) Spam Protection | Automatic Updates (M, H)

Automatically update spam protection mechanisms daily or when updates are made available from product vendor.

2.9 SI-10 Information Input Validation (M, H)

Check the validity of the following information inputs: character set, length, numerical range, and acceptable values to verify that inputs match specified definitions for format and content as it relates to both manual user inputs and automated inputs.

2.10 SI-11 Error Handling (M, H)

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to authorized ED personnel.

2.11 SI-12 Information Management and Retention (P, L, M, H)

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

2.11.1 SI-12(1) Information Management and Retention | Limit Personally Identifiable Information Elements (P)

Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: approved elements of personally identifiable information.

2.11.2 SI-12(2) Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research (P)

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: Approved techniques such as collecting the minimum identity data needed; de-identifying data as soon as possible after collection and/or separating data elements into a coded data set and an identity-only data set; using encryption if identifiable information is:

a. stored on a networked computer or device;

b. transmitted over a network; and/or

c. stored on a removable medium (e.g., laptop computer or a USB flash drive); and limiting access to personally identifiable information.

2.11.3 SI-12(3) Information Management and Retention | Information Disposal (P)

Use the following techniques to dispose of, destroy, or erase information following the retention period: in accordance with the current version of NIST SP 800-88.

2.12 SI-16 Memory Protection (M, H)

Implement the following controls to protect the system memory from unauthorized code execution: ED approved security safeguards to include but not limited to the use of either hardware or software-based data execution prevention and address space layout randomization.

2.13 SI-18 Personally Identifiable Information Quality Operations (P)

a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle at least annually (i.e., each fiscal year); and

b. Correct or delete inaccurate or outdated personally identifiable information.

2.13.1 SI-18(4) Personally Identifiable Information Quality Operations | Individual Requests (P)

Correct or delete personally identifiable information upon request by individuals or their designated representatives.

2.14 SI-19 De-identification (P)

a. Remove the following elements of personally identifiable information from datasets: PII and Sensitive PII; and

b. Evaluate at least annually (i.e., each fiscal year) for effectiveness of de-identification.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: ACRONYMS

Table 2: Acronym List

Acronym	Description
ACS	Administrative Communications System
AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSF	Cyber Security Framework
DHS	Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting & Conformance
ED	Department of Education
EDSOC	Department of Education Security Operations Center
EO	Executive Order
FIPS	Federal Information Processing Standard
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OS	Operating System
PAM	Privileged Account Management
PII	Personally Identifiable Information
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SPF	Sender Policy Framework

APPENDIX B: BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray and notated with an asterisk.

Table 3: Baseline Control Parameter Summary

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SI-1	Policy and Procedures	x	x	x	x	ID.GV, DE.DP	ID.GV-1, ID.GV-3, DE.DP-2
SI-2	Flaw Remediation		x	x	x	ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status			x	x	ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
*SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
*SI-2(4)	Flaw Remediation | Automated Patch Management Tools					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
*SI-2(5)	Flaw Remediation | Automatic Software and Firmware Updates					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
*SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software and Firmware					ID.RA, PR.IP, PR.PO-P	ID.RA-1, PR.IP-12, PR.PO-P10
SI-3			x	x	x	DE.CM, DE.DP	DE.CM-4, DE.DP-3
*SI-3(4)	Malicious Code Protection | Updates Only by Privileged Users					DE.CM, DE.DP	DE.CM-4, DE.DP-3
*SI-3(6)	Malicious Code Protection | Testing and Verification					DE.CM, DE.DP	DE.CM-4, DE.DP-3
*SI-3(8)	Malicious Code Protection | Detect Unauthorized Commands					DE.CM, DE.DP	DE.CM-4, DE.DP-3
*SI-3(10)	Malicious Code Protection | Malicious Code Analysis					DE.CM, DE.DP	DE.CM-4, DE.DP-3
SI-4	System Monitoring		x	x	x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(1)	System Monitoring | System-wide Intrusion Detection System					ID.RA, PR.DS, PR.IP, DE.AE,	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis			x	x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(3)	System Monitoring | Automated Tool and Mechanism Integration					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic			x	x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(5)	System Monitoring | System-generated Alerts			x	x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(7)	System Monitoring | Automated Response to Suspicious Events					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(9)	System Monitoring | Testing of Monitoring Tools and Mechanisms					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(10)	System Monitoring | Visibility of Encrypted Communications				x	ID.RA, PR.DS, PR.IP,	ID.RA-1, PR.DS-5, PR.IP-8,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(12)	System Monitoring | Automated Organization-generated Alerts				x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(13)	System Monitoring | Analyze Traffic and Event Patterns					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(14)	System Monitoring | Wireless Intrusion Detection				x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(15)	System Monitoring | Wireless to Wireline Communications					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(16)	System Monitoring | Correlate Monitoring Information					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(17)	System Monitoring | Integrated Situational Awareness					ID.RA, PR.DS,	ID.RA-1, PR.DS-5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(19)	System Monitoring | Risk for Individuals					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(20)	System Monitoring | Privileged Users				x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(21)	System Monitoring | Probationary Periods					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-4(22)	System Monitoring | Unauthorized Network Services				x	ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(23)	System Monitoring | Host-based Devices					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
*SI-4(24)	System Monitoring | Indicators of Compromise					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
*SI-4(25)	System Monitoring | Optimize Network Traffic Analysis					ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, PR.PO-P, PR.DS-P	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, PR.PO-P6, PR.DS-P5
SI-5	Security Alerts, Advisories, and Directives		x	x	x	ID.RA, RS.CO, RS.AN	ID.RA-1, ID.RA-2, ID.RA-3, RS.CO-5, RS.AN-5
SI-5(1)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories				x	ID.RA, RS.CO, RS.AN	ID.RA-1, ID.RA-2, ID.RA-3, RS.CO-5, RS.AN-5
SI-6	Security and Privacy Function Verification				x	CT.DM-P	CT.DM-P9
*SI-6(2)	Security and Privacy Function Verification | Automation Support for Distributed Testing					CT.DM-P	CT.DM-P9
*SI-6(3)	Security and Privacy Function Verification | Report Verification Results					CT.DM-P	CT.DM-P9
SI-7	Software, Firmware, and Information Integrity			x	x	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks			x	x	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations				x	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(3)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations				x	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response			X	X	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication				x	PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(16)	Software, Firmware, and Information Integrity | Time Limit on Process Execution Without Supervision					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
*SI-7(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection					PR.DS, PR.DS-P	PR.DS-6, PR.DS-P6
SI-8	Spam Protection			x	x	DE.CM	DE.CM-4
SI-8(2)	Spam Protection | Automatic Updates			X	X	DE.CM	DE.CM-4
*SI-8(3)	Spam Protection | Continuous Learning Capability					DE.CM	DE.CM-4
SI-10	Information Input Validation			x	x	PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(1)	Information Input Validation | Manual Override Capability					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(2)	Information Input Validation | Review and Resolve Errors					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(3)	Information Input Validation | Predictable Behavior					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(4)	Information Input Validation | Timing Interactions					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
*SI-10(6)	Information Input Validation | Injection Prevention					PR.DS, CT.DM-P, PR.DS-P	PR.DS-6, CT.DM-P6, PR.DS-P6
SI-11	Error Handling			x	x		
SI-12	Information Management and Retention	x	x	x	x	CT.PO-P, CT.DM-P, CT.DP-P	CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2
SI-12(1)	Information Management and Retention | Limit Personally Identifiable Information Elements	x				CT.PO-P, CT.DM-P, CT.DP-P	CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
SI-12(2)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	x				CT.PO-P, CT.DM-P, CT.DP-P	CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2
SI-12(3)	Information Management and Retention | Information Disposal	x				CT.PO-P, CT.DM-P, CT.DP-P	CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2
*SI-13	Predictable Failure Prevention						
*SI-13(1)	Predictable Failure Prevention | Transferring Component Responsibilities						
*SI-13(3)	Predictable Failure Prevention | Manual Transfer Between Components						
*SI-13(4)	Predictable Failure Prevention | Standby Component Installation and Notification						
*SI-13(5)	Predictable Failure Prevention | Failover Capability						
*SI-14	Non-persistence						
*SI-14(1)	Non-persistence | Refresh from Trusted Sources						
*SI-14(2)	Non-persistence | Non-persistent Information						
*SI-14(3)	Non-persistence | Non-persistent Connectivity						
*SI-15	Information Output Filtering						
SI-16	Memory Protection			x	x		
*SI-17	Fail-safe Procedures						
SI-18	Personally Identifiable Information Quality Operations	x				GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8
*SI-18(1)	Personally Identifiable Information Quality Operations | Automation Support					GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8
SI-18(2)	Personally Identifiable Information Quality Operations | Data Tags					GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
							CM.AW-P6, CM.AW-P8
SI-18(3)	Personally Identifiable Information Quality Operations | Collection					GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8
SI-18(4)	Personally Identifiable Information Quality Operations | Individual Requests	x				GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8
*SI-18(5)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion					GV.MT-P, CT.PO-P, CT.DM-P, CM.AW-P	GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8
SI-19	De-identification	x				GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(1)	De-identification | Collection					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(2)	De-identification | Archiving					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(3)	De-identification | Release					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(4)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(5)	De-identification | Statistical Disclosure Control					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(6)	De-identification | Differential Privacy					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-19(7)	De-identification | Validated Algorithms and Software					GV.MT-P, CT.DM-P,	GV.MT-P5, CT.DM-P9,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
						CT.DP-P	CT.DP-P2, CT.DP-P3
*SI-19(8)	De-identification | Motivated Intruder					GV.MT-P, CT.DM-P, CT.DP-P	GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3
*SI-20	Tainting						
*SI-21	Information Refresh						
*SI-22	Information Diversity						
*SI-23	Information Fragmentation						