FR 1400C

OMB No. 7100-0180
Approval Expires May 2022

Offeror Questionnaire

The Offeror shall complete the entire questionnaire for the application that will be used to meet the requirements of the solicitation that processes, stores and/or transmits data from Board of Governors of the Federal Reserve System. The questions below refer to the specific application's controls. The Offeror shall enter answers on Columns C and D. If the control does not apply, select "Other" AND enter in a comment (required).

For guidance on each question, reference the control on Column E in NIST SP 800-53 r4 publication. *Link to NIST 800-53 r4 Publication*

Solicitation Number:

Title:

Control/Control Questions	**Selection Options** ***Enter Response in Column C & D***	**Offeror's Response**	**Offeror's Response Explanation/File Name**
ACCESS CONTROL			
AC-2	Low		
Do you permit the use of guest or anonymous type accounts?	1-no 2-other 3-yes		
Do you disable or change the default password for default accounts?	1- yes 2-other 3-no		
Do you allow for group level access? If yes, please explain design criteria	1-no 2-other 3-yes		
Do you require a designated individual to approve account creation?	1-no 2-other 3-yes		
Do you have a repeatable process for activating, modifying, disabling, and removing accounts?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you guarantee the deactivation of inactive accounts within a set period of time?	1-yes, 180 days 2-yes, <180 days 3-other 4-no		
Do you periodically review system accounts and provide customers with a list of accounts to review?	1-yes 2-no 3-explain		
AC-3	Low and Moderate		
Do you have the capability to limit access to the information system or service?	1-yes 2-other 3-no		
Do you limit access privileges on accounts?	1-yes 2-other 3-no		
AC-7	Low and Moderate		
Do you automatically suspend accounts after a maximum number of unsuccessful login attempts?	1-yes 2-other 3-no		
Do you require an administrator-level user to unlock suspended accounts?	1-yes 2-other 3-no		
AC-8	Low and Moderate		
Do you have the capability to display a customized system usage notification for the Federal Reserve Board?	1-yes 2-other 3-no		
AC-14	Low and Moderate		
Are users given access without authentication? If yes, please explain.	1-no 2-other 3-yes		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Are the actions of an unauthenticated user only extended to necessary functions?	1-n/a 2-yes 3-other 4-no		
AC-17	Low		
Do you authorize and monitor remote access to your systems?	1-no 2-other 3-yes		
AC-18	Low		
Do you deploy wireless network access?	1-no 2-other 3-yes		
If so, do you monitor for unauthorized access and enforce requirements for connectivity?	1-yes 2-other 3-no		
AWARENESS TRAINING			
AT-2, AT-3 & AT-4	Low and Moderate		
Do you require your employees to go through security awareness training?	1-yes 2-other 3-no		
If so, is the training based on an employee's role in the organization?	1-yes 2-other 3-no		
Do you keep records of employee training?	1-yes 2-other 3-no		
AUDIT AND ACCOUNTABILITY			
AU-2	Low		
Do you generate audit records that identify users and when they accessed the information system or service?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you generate audit records that identify users and when they accessed the application?	1-yes 2-other 3-no		
Do you generate audit records that identify unauthorized access attempts to your service/system?	1-yes 2-other 3-no		
Do you generate audit records that identify failed access attempts to your application?	1-yes 2-other 3-no		
AU-3	Low		
Do the audit records for your system/service contain information to establish what event occurred, when (date and time) the event occurred, where the event occurred, the sources of the event, the success or failure of the event, and the identity of subjects associated with the event?	1-yes 2-other 3-no		
Do the audit records for your application contain information to establish what event occurred, when (date and time) the event occurred, where the event occurred, the sources of the event, the success or failure of the event, and the identity of subjects associated with the event?	1-yes 2-other 3-no		
AU-4	Low and Moderate		
Do you have audit record storage capacity to maintain audit records for your system/service?	1-yes 2-other 3-no		
If yes, for what length of time?	1-more than 12 months 2-12 months 3-less than 12 months		
Do you have audit record storage capacity to maintain audit records for your application?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
If yes, for what length of time?	1-more than 12 months 2-12 months 3-less than 12 months		
AU-5	Low and Moderate		
Do you create alerts in the event of an audit processing failure in your system/service?	1-yes 2-other 3-no		
Do you create alerts in the event of an audit processing failure in your application?	1-yes 2-other 3-no		
Does log rotation take place for your system/service to prior to truncation or overwriting?	1-yes 2-other 3-no		
Does log rotation take place for your application to prior to truncation or overwriting?	1-yes 2-other 3-no		
AU-6	Low and Moderate		
Are review and analysis conducted on system audit records for inappropriate or unusual activity?	1-yes 2-other 3-no		
If so, what is the frequency?	1-daily 2-weekly 3-monthly 4-other		
Are review and analysis conducted on application audit records for inappropriate or unusual activity?	1-yes 2-other 3-no		
If so, what is the frequency?	1-daily 2-weekly 3-monthly 4-other		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you deploy automated mechanisms to integrate audit reviews, analysis, and reporting?	1-yes 2-other 3-no		
Are audit records across different repositories correlated and reviewed to gain a better understanding of system-wide events?	1-yes 2-other 3-no		
AU-8	Low		
Do you use a common system clock for deployed information systems?	1-yes 2-other 3-no		
AU-9	Low		
Do you have protections in place to prevent unauthorized access to audit information?	1-yes 2-other 3-no		
If so, please explain the controls.	answer in column D		
AU-11	Low and Moderate		
Do you maintain audit records online for a minimum of four weeks and offline for a minimum of a year?	1-yes 2-other 3-no		
AU-12	Low and Moderate		
Do you provide a centralized audit repository that allows for event correlation and by-system reporting?	1-yes 2-other 3-no		
SECURITY ASSESSMENT AND AUTHORIZATION			
CA-2	Low		
Do you have a security assessment plan that determines security control effectiveness and that produces an appropriate mitigation plan from the results of the assessment?	1-yes 2-other 3-no		
CA-3	Low		
Do you create contractual agreements for your third-party service providers?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Are your third-party service providers' system connections documented with the interface characteristics, security requirements, and the nature of the communication?	1-yes 2-other 3-no		
Are system connections monitored for enforcement of security requirements?	1-yes 2-other 3-no		
CA-5	Low and Moderate		
Do you develop plans of action and milestones for remediation of deficiencies and weaknesses identified in your systems?	1-yes 2-other 3-no		
CA-6	Low and Moderate		
Do you employ a senior-level executive or manager to ensure effective risk management?	1-yes 2-other 3-no		
CA-7	Low		
Do you apply continuous monitoring for configuration management and for security control assessment of your systems?	1-yes 2-other 3-no		
CA-9	Low and Moderate		
Do you document interconnections with the interface characteristics and security requirements for all system connections?	1-yes 2-other 3-no		
CONFIGURATION MANAGEMENT			
CM-2	Low		
Do you have and maintain a documented baseline configuration for each type of system?	1-yes 2-other 3-no		
CM-4	Low and Moderate		
Do you have qualified security professionals conduct security impact analyses for changes to systems?	1-yes 2-other 3-no		
CM-6	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you implement mandatory configuration settings for systems and software using approved security configuration checklists?	1-yes 2-other 3-no		
If mandatory configurations are not followed, are these exceptions documented and maintained?	1-yes 2-other 3-no		
Do you deploy detection mechanisms for the monitoring of unauthorized changes to a system?	1-yes 2-other 3-no		
CM-7	Low		
Do you configure your systems to provide only essential capabilities and specifically prohibit or restrict the use of unnecessary functions, ports, protocols, and/or services?	1-yes 2-other 3-no		
CM-8	Low		
Do you develop, document, review, and update an inventory of your systems?	1-yes 2-other 3-no		
CONTINGENCY PLANNING			
CP-2	Low		
Do you create contingency plans that include recovery objectives and restoration priorities?	1-yes 2-other 3-no		
Do you have documented contingency roles and responsibilities?	1-yes 2-other 3-no		
Do you revise the contingency plans to address changes and problems encountered during contingency plan implementation and testing?	1-yes 2-other 3-no		
CP-3	Low and Moderate		
Do you provide contingency training to your staff on a minimum annual basis?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
CP-4	Low		
Do you test contingency plans on a minimum annual basis?	1-yes 2-other 3-no		
Do you review the contingency plan test results, and identify and take corrective actions?	1-yes 2-other 3-no		
CP-9	Low		
Do you back up user-level information?	1-yes 2-other 3-no		
Do you back up system-level information?	1-yes 2-other 3-no		
Do you protect the integrity of the backup information?	1-yes 2-other 3-no		
Is at least one copy of the backup information stored in a secure offsite location?	1-yes 2-other 3-no		
CP-10	Low		
Are systems recovered or reconstituted to a known state after a disruption, compromise, or failure?	1-yes 2-other 3-no		
IDENTIFICATIION AND AUTHENTICATION			
IA-2	Low		
Do privileged accounts require multifactor authentication?	1-yes 2-other 3-no		
IA-4	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you require authorization prior to the creation of user accounts?	1-yes 2-other 3-no		
Is each user or device assigned a unique identifier?	1-yes 2-other 3-no		
Are identifiers prevented from re-use for a defined time period after being disabled?	1-yes 2-other 3-no		
Are identifiers disabled after a period of inactivity?	1-yes 2-other 3-no		
Are identifiers deleted when no longer required?	1-yes 2-other 3-no		
IA-5	Low		
Do you have a mechanism to verify a party upon the initial authenticator/credential distribution?	1-yes 2-other 3-no		
Do you have an established and implemented procedure for initial authenticator/credential distribution, for lost/compromised or damaged authenticators/credentials, and for revoking authenticators/credentials?	1-yes 2-other 3-no		
Do you change default password and settings of authenticators/credentials upon system installation?	1-yes 2-other 3-no		
Do you have minimum and maximum lifetime restrictions and re-use conditions on authenticators/credentials?	1-yes 2-other 3-no		
Do you protect authenticator/credential content from unauthorized disclosure and modification?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you enforce minimum password complexity?	1-yes 2-other 3-no		
Do you encrypt passwords in storage and in transmission?	1-yes 2-other 3-no		
If multi-factor authentication is offered, does the authentication assurance level meet that of NIST 800-63 Level 4 authentication?	1-yes 2-other 3-no		
IA-6	Low and Moderate		
Do you obscure feedback information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals?	1-yes 2-other 3-no		
Do you obscure feedback information during the authentication process to protect the application from possible exploitation/use by unauthorized individuals?	1-yes 2-other 3-no		
IA-7	Low and Moderate		
What cryptologic algorithms are used by your system?	answer in column D		
Are they FIPS 140-2 compliant?	1-yes 2-other 3-no		
What cryptologic algorithms are used by your application?	answer in column D		
Are they FIPS 140-2 compliant?	1-yes 2-other 3-no		
IA-8	Low and Moderate		
Will non-Federal Reserve Board systems and users that connect to the Federal Reserve Board system be uniquely identified?	1-yes 2-other 3-no		
Does the information system accept and electronically verify Personal Identity Verification Interoperability (PIV-I) credentials?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
INCIDENT RESPONSE			
IR-2	Low and Moderate		
Do you train personnel in incident response roles and responsibilities?	1-yes 2-other 3-no		
Do you provide refresher training for incident response?	1-yes 2-other 3-no		
IR-4	Low		
During contingency planning activities, are incident-handling processes addressed?	1-yes 2-other 3-no		
IR-6	Low and Moderate		
Do your personnel report suspected security incidents to designated authorities within an established timeframe?	1-yes 2-other 3-no		
IR-7	Low and Moderate		
Will you report security incidents to the Federal Reserve Board within a timeframe based on the severity of the incident?	1-yes 2-other 3-no		
Will you ask the Federal Reserve Board for assistance in mitigating the security incident?	3-no 2-other 1-yes		
IR-8	Low and Moderate		
Do you have an established incident response plan that defines reportable incidents, provides metrics for measuring, and provides a roadmap for implementing incident responses?	1-yes 2-other 3-no		
Do you periodically review the incident response plan and address any necessary changes or updates to the plan?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Is the updated plan communicated to the appropriate personnel?	1-yes 2-other 3-no		
MAINTENANCE			
MA -2	Low and Moderate		
Is all equipment maintenance documented, reviewed, and approved prior to implementation of any changes?	1-yes 2-other 3-no		
Is equipment sanitized prior to removal from the facility?	1-yes 2-other 3-no		
Are security controls checked after a repair or change made during maintenance?	1-yes 2-other 3-no		
Do your maintenance records include the following?	1-yes 2-other 3-no		
1. Date and time of maintenance	1-yes 2-other 3-no		
2. Name of the individual(s) preforming the maintenance	1-yes 2-other 3-no		
3. Name of escort, if necessary	1-yes 2-other 3-no		
4. Description of the maintenance performed	1-yes 2-other 3-no		
5. A list of equipment or components that are removed or replaced	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
MA-4	Low		
Do you allow remote maintenance?	1-no 2-other 3-yes		
Do you authorize, monitor, and control remote maintenance activities?	1-yes 2-other 3-no		
Do you terminate all sessions and network connections once remote maintenance is complete?	1-yes 2-other 3-no		
MA-5	Low and Moderate		
Do you have a process that authorizes and maintains a list of authorized personnel and organizations for maintenance activities?	1-yes 2-other 3-no		
Do you have a process that ensures the personnel performing the maintenance have the required access authorizations?	1-yes 2-other 3-no		
MEDIA PROTECTION			
MP-2	Low and Moderate		
Do you restrict access to sensitive or classified information to those individuals having a need to know?	1-yes 2-other 3-no		
MP-4	Low		
Do you have automated mechanisms to restrict access to media storage areas and audit access attempts to the media against access that has been granted?	1-yes 2-other 3-no		
MP-5	Low		
Do you document all transports of media into or out of the operational facilities?	1-yes 2-other 3-no		
MP-6	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you sanitize digital and non-digital media prior to disposal or for release out of your control?	1-yes 2-other 3-no		
MP- 7	Low and Moderate		
Do you prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner?	1-yes 2-other 3-no		
PHYSICAL AND ENVIRONMENTAL PROTECTION			
PE-2	Low and Moderate		
Do you develop and maintain lists of authorized personnel that have access to the facility(s) and any restricted parts of the environment?	1-yes 2-other 3-no		
Do you issue authorization credentials for restricted, information system, and communication areas?	1-yes 2-other 3-no		
Are access lists and authorization credentials reviewed at least annually?	1-yes 2-other 3-no		
PE-3	Low and Moderate		
Do you enforce physical access authorization for all physical access points?	1-yes 2-other 3-no		
Do you verify individual access authorizations before granting access to the facility?	1-yes 2-other 3-no		
Does your facility have controlled entry points that use physical access devices and/or guards?	1-yes 2-other 3-no		
Do you authenticate visitors before allowing access to a facility that is not designated for public access?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Are visitors to the facility escorted and their activities monitored?	1-yes 2-other 3-no		
Do you change keys and combinations to the relevant access point of the facility upon the loss or compromise of the access point to the facility(s), or in the event of an employee or contractor transfer or termination?	1-yes 2-other 3-no		
PE-6	Low		
Do you monitor physical access and respond to physical security incidents?	1-yes 2-other 3-no		
Do you review physical access logs?	1-yes 2-other 3-no		
Are physical access events incorporated into incident response plans?	1-yes 2-other 3-no		
PE-8	Low and Moderate		
Do you maintain visitor access records to the facility(s) and are these records reviewed on at least a quarterly basis?	1-yes 2-other 3-no		
PE-12	Low and Moderate		
Does the facility have emergency lighting for the loss or disruption of electrical power?	1-yes 2-other 3-no		
PE-13	Low		
Do you have fire detection devices arranged in zones with remote monitoring for fire suppression?	1-yes 2-other 3-no		
PE-14	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Does the facility employ automated mechanisms to monitor and maintain temperature and humidity levels?	1-yes 2-other 3-no		
PE-15	Low and Moderate		
Does the facility protect information systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and at locations known to key personnel?	1-yes 2-other 3-no		
PE-16	Low and Moderate		
Do you control, authorize, and monitor information system component hardware and devices entering and exiting the facility and maintain records for those items?	1-yes 2-other 3-no		
PLANNING			
PL-2	Low		
Do you create an individualized security plan for each information system or service hosted or executed at your facilities?	1-yes 2-other 3-no		
Do you own and maintain the controls that are documented in the security plan for each hosted information system or service?	1-yes 2-other 3-no		
PL-4	Low		
Have you established rules that govern users on expected behavior with regard to information and information system usage, and do the users sign an acknowledgement indicating that they have read, understand, and agree to abide by the rules?	1-yes 2-other 3-no		
PERSONNEL SECURITY			
PS-2	Low and Moderate		
Do you assign risk designations and establish screening criteria for positions in your organization?	1-yes 2-other 3-no		
PS-3	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you conduct background checks including credit reports prior to employment and recheck the employee or contractor within a two-year period?	1-yes 2-other 3-no		
PS-4	Low and Moderate		
Upon termination of an employee or contractor do you conduct exit interviews, immediately terminate access to systems, and retrieve all security-related information and documentation?	1-yes 2-other 3-no		
PS-5	Low and Moderate		
Upon the transfer of an employee or contractor, do review the logical and physical access authorizations to verify that the authorizations are still appropriate?	1-yes 2-other 3-no		
PS-6	Low and Moderate		
Do you require employees and contractors to sign access agreements that are reviewed on a periodic basis?	1-yes 2-other 3-no		
PS-7	Low and Moderate		
Have you established security requirements for third-party personnel that are included in contracts that require your providers to follow the established security criteria and requirements of your organization?	1-yes 2-other 3-no		
PS-8	Low and Moderate		
Are employees and contractors required to adhere to security policies in which non-adherence is subject to disciplinary action, up to and including termination and/or civil or criminal liability?	1-yes 2-other 3-no		
RISK ASSESSMENT			
RA-2	Low and Moderate		
Do you have a documented information system categorization policy that establishes how processing, storage, and transmission of information will be conducted and maintained?	1-yes 2-other 3-no		
RA-3	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you conduct information system risk assessments that include the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of an information system?	1-yes 2-other 3-no		
Do you document, review, and update information system risk assessments on a periodic basis?	1-yes 2-other 3-no		
RA-5	Low		
Do you conduct frequent scans for vulnerabilities on information systems and hosted applications?	1-yes 2-other 3-no		
Do you analyze vulnerability scan reports and results, taking appropriate actions for remediation in the appropriate amount of time?	1-yes 2-other 3-no		
SYSTEM AND SERVICE ACQUISITION			
SA-2	Low and Moderate		
Do you have processes and/or procedures for determining information security requirements and the allocation of security resources on a minimum annual basis for your information system?	1-yes 2-other 3-no		
SA-3	Low and Moderate		
Do you deploy a system development lifecycle methodology that includes security considerations and identifies necessary system security roles and responsibilities for your information system?	1-yes 2-other 3-no		
SA-4	Low		
Are security attributes both implicit and explicit taken into consideration in the acquisition of equipment?	1-yes 2-other 3-no		
Do you explicitly assign information systems or services to a specific owner?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
SA-5	Low and Moderate		
Do you have explicit security documentation on the components, configuration, and settings for an information system for the purposes of installation, review, and testing?	1-yes 2-other 3-no		
SA-9	Low		
Do you require external service providers to adhere to information security requirements?	1-yes 2-other 3-no		
Are external service providers contractually obligated to meet particular service levels?	1-yes 2-other 3-no		
SYSTEM AND COMMUNICATION PROTECTION			
SC-5	Low and Moderate		
Do you employ 'content filtering' mechanisms (e.g., packet filtering, system redundancy, increased bandwidth capacity) to prevent denial of service attacks?	1-yes 2-other 3-no		
SC -7	Low		
Do you have policies in place to monitor and control external/internal network connections?	1-yes 2-other 3-no		
Do you have monitoring devices at these connection points?	1-yes 2-other 3-no		
SC-12	Low and Moderate		
Do you have a process in place to manage cryptographic logic keys for your system/service?	1-yes 2-other 3-no		
Do you have a process in place to manage cryptographic logic keys for your application?	1-yes 2-other 3-no		
SC-13	Low and Moderate		

Control/Control Questions	Selection Options *Enter Response in Column C & D*	Offeror's Response	Offeror's Response Explanation/File Name
Do you use cryptology to protect information?	1-yes 2-other 3-no		
Do you use cryptology to protect applications?	1-yes 2-other 3-no		
SC-15	Low and Moderate		
Do you employ a policy to prevent the remote connection of collaborative devices?	1-yes 2-other 3-no		
SC-18	Low and Moderate		
Do you have a policy in place for the use of mobile code?	1-yes 2-other 3-no		
Do you have a Certification Authority for issuance of mobile code technology certificates?	1-yes 2-other 3-no		
SC-22	Low and Moderate		
Do you employ a name/address resolution solution in your network architecture?	1-yes 2-other 3-no		
SC-39	Low and Moderate		
Does the information system maintain a separate execution domain for each executing process?	1-yes 2-other 3-no		
Please describe how this is accomplished.	answer in column D		
SYSTEM AND INFORMATION INTEGRITY			
SI-2	Low		
Do you employ a process for flaw remediation in information systems?	1-yes 2-other 3-no		

Control/Control Questions	Selection Options	Offeror's	Offeror's Response
	Enter Response in Column C & D	Response	Explanation/File Name
Do you employ a process for flaw remediation in your application?	1-yes 2-other 3-no		
SI-3	Low		
Do you employ a mechanism to prevent and detect malicious code on information systems?	1-yes 2-other 3-no		
SI-4	Low and Moderate		
Do you employ a mechanism to monitor for attacks on information systems?	1-yes 2-other 3-no		
Do you monitor for unauthorized use of information systems?	1-yes 2-other 3-no		
Do you deploy intrusion monitoring tools?	1-yes 2-other 3-no		
SI-5	Low and Moderate		
Do you have a process to receive, generate, and disseminate security alerts, advisories, and directives from designated external organizations?	1-yes 2-other 3-no		
SI-12	Low and Moderate		
Do you have a process or procedure in place to ensure the output of information systems or services is properly handled based on data classification?	1-yes 2-other 3-no		