Executive Order 13556 Impact Assessment for the Data Management Office (DMO)

DM-2016-POL-0001

January 2, 2017

Version 1.0

Contents

Background 3

Governance 3

Policy 3

Training 3

Technology 3

Self-Inspection 4

Additional Impact 4

Security Families 5

- Access Control 5
- Awareness and Training 6
- Audit and Accountability 6
- Configuration Management 7
- Identification and Authorization 7
- Incident Response 8
- Maintenance 8
- Personnel Security 9
- Physical Protection 9
- Risk Assessment 9
- Security Assessment 9
- System and Communication Protection 10
- System and Information Integrity 10

Executive Order 13556

Impact to New York State of New York

Background

The Executive Order 13556 (EO 13556) standardizes the way in which departments and agencies (agencies) handle unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies. The Order establishes the CUI program and designates the National Archives and Records Administration as its Executive Agent (EA). Successful implementation of this Order by agencies will enhance the efficient and effective management, control, and sharing of CUI and further the administration's goals of openness and uniformity of government practices. A standardized program that is consistently applied will support the individual missions of agencies and will enhance information sharing within and between agencies as well with State, local, tribal, and private sector partners.

The following are specific areas within Information Technology Service's (ITS) scope where EO 13556 affects New York State (NYS) information technology (IT) portfolios, programs, projects, and activities.

Governance

- Identify Senior Agency Official, and other designated CUI points of contact.
- Define roles and responsibilities and describe agency-level processes established to guide and direct the program and its requirements per the Order and Notice.

Policy

- Describe agency-level plans and target dates for creating and promulgating CUI policies and procedures including safeguarding, dissemination, marking, decontrol, and dispute resolution.

Training

- Identify all affected personnel requiring training.
- Describe agency-level development plans to ensure that personnel who create or handle CUI have a satisfactory knowledge and understanding of relevant CUI categories and associated markings, applicable safeguarding, dissemination, and decontrol policies and procedures.
- Describe plans for tailoring initial and refresher training to meet the specific needs of the agency and the activities that personnel are expected to perform as determined by the individual agency.
- Describe the means, methods, and frequency of CUI training.
- Provide proposed dates for launching training.

Technology

- Describe efforts to review Information Technology systems and toolsets to identify systems impacted by CUI.

- Describe plans for electronic marking solutions (if applicable).
- Propose target dates for phased implementation.

Self-Inspection

- Describe agency-level plans and target dates for the creation of a self-inspection program including reviews and assessments, to evaluate program effectiveness, measure the level of compliance with the Order and Notice, and monitor the progress of CUI implementation.
- Describe plans to integrate lessons learned from reviews and assessments to improve operational policies, procedures, and training, establish a system for corrective action to prevent and respond to non-compliance with the Order and Notice.
- Provide documentation that reflects the analysis and conclusions of the self-inspection program to the EA on an annual basis and as requested by the EA.

Additional Impact

- Work with NARA or other federal agency to ensure that federal records are appropriately classified in NYS systems.
- Coordinate with NARA to learn what training NYS could leverage to ensure that State personnel understand the rules for each dataset within NYS possession.
- Probably have to produce an EO 13556 compliance plan at some point and have on file when federal government audits their data.
- NYS will be responsible for ensuring IT systems understand and respect security markings on data.
- NYS will need to develop a documented data sharing (request, review, and approval) process that agencies will have to follow relative to using CUI data.

Overview

The following represent *security families* identified by the National Institute of Standards and Technology (NIST) as part of *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* guidance. Each section shows specific requirements and an assessment in terms of ITS roles and responsibilities. *Joint* ownership refers to work performed jointly between the Data Management Office (DMO) and the Information Security Office (ISO).

Security Families

FAMILY	OWNER	FAMILY	OWNER
Access Control	Joint	Media Protection	Joint
Awareness and Training	Joint	Personnel Security	Joint
Audit and Accountability	Joint	Physical Protection	Joint
Configuration Management	Joint	Risk Assessment	Security
Identification and Authentication	Joint	Security Assessment	Security
Incident Response	Joint	System and Communications Protection	Joint
Maintenance	Joint	System and Information Integrity	Joint

Access Control

Basic Security Requirement	Owner
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Security
Derived Security Requirement	Security
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Security
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Security
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Security
3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	Security
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Security
3.1.8 Limit unsuccessful logon attempts.	Security
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	Joint
3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Security
3.1.11 Terminate (automatically) a user session after a defined condition.	Security
3.1.12 Monitor and control remote access sessions.	Security
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Security
3.1.14 Route remote access via managed access control points.	Security

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Joint
3.1.16 Authorize wireless access prior to allowing such connections.	Joint
3.1.17 Protect wireless access using authentication and encryption.	Security
3.1.18 Control connection of mobile devices.	Security
3.1.19 Encrypt CUI on mobile devices.	Security
3.1.20 Verify and control/limit connections to and use of external information systems.	Joint
3.1.21 Limit use of organizational portable storage devices on external information systems.	Joint
3.1.22 Control information posted or processed on publicly accessible information systems.	Security

Awareness and Training

Basic Security Requirement	Owner
3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	Joint
3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	Joint
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Security

Audit and Accountability

Basic Security Requirement	Owner
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Joint
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Security
Derived Security Requirement	
3.3.3 Review and update audited events.	Joint
3.3.4 Alert in the event of an audit process failure.	Security
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Security
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.	Security
3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Security
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	Security
3.3.9 Limit management of audit functionality to a subset of privileged users	Security

Configuration Management

Basic Security Requirement	Owner
3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Joint
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Security
Derived Security Requirement	
3.4.3 Track, review, approve/disapprove, and audit changes to information systems.	Security
3.4.4 Analyze the security impact of changes prior to implementation.	Joint
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Joint
3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Security
3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Security
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Security
3.4.9 Control and monitor user-installed software.	Security

Identification and Authorization

Basic Security Requirement	Owner
3.5.1 Identify information system users, processes acting on behalf of users, or devices.	Joint
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Joint
Derived Security Requirement	
3.5.3 Use multifactor authentication for local and network access23 to privileged accounts and for network access to non-privileged accounts.	Security
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Security
3.5.5 Prevent reuse of identifiers for a defined period.	Security
3.5.6 Disable identifiers after a defined period of inactivity.	Security
3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.	Security
3.5.8 Prohibit password reuse for a specified number of generations.	Security
3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.	Security
3.5.10 Store and transmit only encrypted representation of passwords.	Security
3.5.11 Obscure feedback of authentication information.	Security

Incident Response

Basic Security Requirement	Owner
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Joint
3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Joint
Derived Security Requirement	
3.6.3 Test the organizational incident response capability.	Security

Maintenance

Basic Security Requirement	Owner
3.7.1 Perform maintenance on organizational information systems.	Security
3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Security
Derived Security Requirement	
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Joint
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Security
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Security
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	Security

Media Protection

Basic Security Requirement	Owner
3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	Joint
3.8.2 Limit access to CUI on information system media to authorized users.	Joint
3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Joint
Derived Security Requirement	
3.8.4 Mark media with necessary CUI markings and distribution limitations.	Joint
3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Security
3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Security
3.8.7 Control the use of removable media on information system components.	Security
3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.	Joint
3.8.9 Protect the confidentiality of backup CUI at storage locations.	Joint

Personnel Security

Basic Security Requirement	Owner
3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.	Joint
3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Security

Physical Protection

Basic Security Requirement	Owner
3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Security
3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.	Security
Derived Security Requirement	
3.10.3 Escort visitors and monitor visitor activity.	Security
3.10.4 Maintain audit logs of physical access.	Joint
3.10.5 Control and manage physical access devices.	Security
3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites)	Joint

Risk Assessment

Basic Security Requirement	Owner
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	Security
Derived Security Requirement	
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	Security
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	Security

Security Assessment

Basic Security Requirement	Owner
3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Security
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	Security
3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Security

System and Communication Protection

Basic Security Requirement	Owner
3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Joint
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	Joint
Derived Security Requirement	
3.13.3 Separate user functionality from information system management functionality.	Security
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	Security
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Joint
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Security
3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	Security
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Security
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Security
3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system.	Security
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Security
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Security
3.13.13 Control and monitor the use of mobile code.	Security
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Security
3.13.15 Protect the authenticity of communications sessions.	Security
3.13.16 Protect the confidentiality of CUI at rest.	Security

System and Information Integrity

Basic Security Requirement	Owner
3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	Security
3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.	Security
3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.	Security
Derived Security Requirement	
3.14.4 Update malicious code protection mechanisms when new releases are available.	Security

3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Security
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Security
3.14.7 Identify unauthorized use of the information system.	Security