OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

Inspection of Federal Computer Security at the U.S. Department of the Interior

Report No.: 2016-ITA-032

August 2016

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

AUG 0 8 2016

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall
Deputy Inspector General

Subject: Final Report – Inspection of Federal Computer Security at the U.S. Department of the Interior
Report No. 2016-ITA-032

This report presents the results of our inspection of Federal Computer Security at the U.S. Department of the Interior (DOI). As required by Section 406 of the Cybersecurity Act of 2015, we inspected DOI's policies, procedures, and practices for securing its computer networks and systems for all covered systems related to:

1. logical access control policies and practices;
2. use of multifactor authentication;
3. software inventory;
4. threat prevention; and
5. contractor oversight.

We found that DOI has implemented measures such as multifactor authentication to reduce the risk of unauthorized access to its covered systems and software inventory management to comply with intellectual property rights and prevent spending public funds on unused software. DOI, however, needs to update its logical access controls to meet current standards to ensure that general users do not have access to privileged functions and that audit trails are in place to monitor actions taken by privileged users to mitigate risk from insider threats. DOI also needs to ensure that its mobile computing devices are encrypted and securely configured to prevent the loss of sensitive data when these devices are lost or stolen. Finally, DOI needs the ability to inspect encrypted traffic for malicious content to prevent the loss of sensitive data. Our report does not contain recommendations because the Act only requires us to describe DOI's policies, procedures, and practices.

We issued this report to the OCIO for informational purposes. The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued. If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief

In accordance with the Cybersecurity Act of 2015, we inspected the U.S. Department of the Interior's (DOI) policies, procedures, and practices for securing its computer networks and systems for all covered systems related to—

1. logical access control policies and practices;
2. use of multifactor authentication;
3. software inventory;
4. threat prevention; and
5. contractor oversight

DOI has implemented many information security measures for access controls, software, threat prevention, and contractor management, but it needs further enhancements. For example, DOI has implemented multifactor authentication to reduce the risk of unauthorized access to its covered systems and software inventory management to comply with intellectual property rights and prevent spending public funds on unused software. DOI, however, needs to update its logical access controls to meet current National Institute of Standards and Technology requirements, which will ensure that general users do not have access to privileged functions and that audit trails are in place to monitor actions taken by privileged users to mitigate risk from insider threats. Further, DOI must ensure that its mobile computing devices are encrypted and securely configured to prevent the loss of sensitive data when these devices are lost or stolen. Finally, DOI needs the ability to inspect encrypted traffic for malicious content to prevent the loss of sensitive data.

Introduction

Objective

Our objective was to report on the U.S. Department of the Interior's (DOI's) security policies, procedures, and practices for all DOI covered systems related to—

1. logical access control policies and practices;
2. use of multifactor authentication;
3. software inventory;
4. threat prevention; and
5. contractor oversight.

Appendix 1 provides further details about our scope and methodology.

Background

In December 2015, the President signed into law the Cybersecurity Act of 2015 (Act). Section 406 of the Act requires that Inspectors General (IGs) submit reports to Congress by August 14, 2016, on information collected for all covered systems. According to the Act, covered systems are national-security systems or Federal systems, to include contractor systems, that provide access to personally identifiable information (PII). DOI reported that it operated 88 covered systems—72 DOI computer systems and 16 contractor computer systems—that provide access to PII. DOI also reported that as of March 31, 2016, it had 71,290 general users and 4,728 privileged users of its computer systems.

The Act requires IGs to report on security policies, procedures, and practices for logical access controls, use of multifactor authentication, software inventory, threat prevention, and contractor oversight.

Logical Access Control Policies and Practices

Logical access refers to controls around the processes of granting or denying requests to obtain and use information systems. The Act requires IGs to provide descriptions of the logical access control policies and practices in place to access covered systems. IGs must also provide a description of the logical access controls used at the Agency to govern access to covered systems by privileged users, which are those users that have elevated access to system control, monitoring, or administrative functions.

Use of Multifactor Authentication

Multifactor authentication is the use of at least two authentication factors to access Federal computer systems and networks. For example, authentication factors may include passwords or personal identification numbers, cryptographic identification devices or tokens, or unique biometric characteristics of the user. The Act requires IGs to provide a description of how

the Agency uses multifactor authentication to govern access to covered systems by privileged users.

Software Inventory

The Act requires IGs to report on the policies and procedures the Agency follows to conduct inventories of software and its licenses present on covered systems.

Threat Prevention

Threat prevention capabilities are used to detect security threats, to include data loss prevention, digital forensics, and digital rights management. The Act requires IGs to report threat prevention capabilities and how the Agency uses them.

Contractor Oversight

The Act requires IGs to report on policies and procedures the Agency uses to ensure that its contractors implement the information security management practices for software inventory and threat prevention.

Results of Review

Logical Access Control Policies and Practices

DOI's logical access control policies and practices require that bureaus follow the National Institute of Standards and Technology (NIST) standards governing both general or privileged user access to information systems containing sensitive data, including PII. According to NIST standards, Federal computer systems that contain PII are categorized as moderate-impact information security systems. This categorization prescribes the minimum controls that must be implemented to help ensure the availability of the computer system, as well as the confidentiality and integrity of the sensitive data it contains. Appendix 2 provides a list and description of the NIST-required minimum logical access controls for a moderate-impact system. DOI's covered systems are categorized as moderate impact.

Eight of the nine systems we tested (seven DOI systems and two contractor systems) did not meet the minimum logical access controls outlined in NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," because DOI has not adopted the current requirements. We compared the logical access controls in the security documentation for the selected systems with the corresponding minimum controls for a moderate-impact computer system.

The systems we reviewed did not document the NIST minimum controls for privileged user accounts, such as—

- restricting privileged accounts to specific personnel so that general users do not have access to privileged functions;
- auditing privileged account functions to help mitigate the risk from insider threats and advanced persistent threats; and
- ensuring that nonprivileged users cannot execute privileged functions to disable, circumvent, or alter implemented security measures.

In addition, these systems did not document controls to ensure the implementation of full-disk encryption on mobile devices, such as smartphones and tablet computers, to protect the confidentiality and integrity of sensitive data.

These deficiencies occurred because DOI has not adopted NIST's current standards and instead is following outdated standards. For example, the logical access controls in the security plans we reviewed were those prescribed by NIST Special Publication 800-53 Revision 3, which was superseded in April 2013 by Revision 4. According to NIST, Federal agencies have up to 1 year from the date of final publication to fully comply with new security standards. The Office of the Chief Information Officer (OCIO) stated that DOI will implement the current logical access controls by December 31, 2016, more than 2 and a half years late.

We also found that these systems did not have documented controls for ensuring the implementation of full-disk encryption on mobile devices, such as smartphones and tablet computers, to protect the confidentiality and integrity of sensitive data. Our June 2016 audit of DOI's mobile computing devices determined that thousands of DOI's mobile computing devices do not have proper security configurations, which could result in unauthorized access to Government systems and data by cybercriminals. Ineffective logical access controls could result in unauthorized access to or modification of DOI computer systems and data, which could have a serious to severe adverse effect on DOI operations and result in the loss of sensitive data.

In addition, in fiscal years 2014 and 2015 Federal Information Security Modernization Act audits, DOI's independent auditor, KPMG, found deficiencies in DOI's logical access practices. For example, DOI has not documented an account management process for granting or removing user access from information systems. DOI also did not timely disable all inactive accounts, increasing the risk of these accounts being used to inappropriately access DOI systems and data. DOI had not performed and documented periodic user account reviews to reduce the risk of users inappropriately obtaining or retaining system access, which could also result in potential compromise of departmental systems and data. KPMG recommended that DOI address deficiencies in its account management practices, and DOI concurred.

Use of Multifactor Authentication

In March 2011, DOI began a Departmentwide roll out of multifactor authentication (PIV card and PIN) for general and privileged user access to DOI computer systems. In September 2015, DOI reported that 100 percent of its computer systems enforce multifactor authentication before granting logical access to privileged users and 92 percent for general users. According to the OCIO, all future computer systems will require multifactor authentication for general and privileged user access. Computer systems that employ multifactor authentication are far more secure than systems secured only by passwords. Many high-profile data breaches, including the 2015 U.S. Office of Personnel Management data breach, could have been prevented with multifactor authentication in place.

Software Inventory

Effective management of software licenses promotes compliance with intellectual property rights and helps ensure that public funds are not spent on unused software. On March 16, 2016, the OCIO issued the Software Asset Management Policy, which mandates that DOI must comply with all software copyrights, license terms, and configurations for software installed on its computers. Further, all unneeded licenses must be eliminated and the procurement of new software licenses is restricted until DOI's needs exceed the number of existing and unused licenses. DOI has drafted a Software Asset Management Guide in order to standardize the methods and processes it uses

to report asset inventories. According to the OCIO, the guide will be finalized in September 2016.

Threat Prevention

DOI's OCIO maintains an Advanced Security Operations Center (ASOC) to provide timely identification, response, and resolution of security incidents that suggest a compromise or potential compromise of DOI networks that could result in the loss of availability, confidentiality, or integrity of systems or data. The ASOC is designed to detect security incidents, such as the installation of malware or denial of service attacks. Moreover, the ASOC provides capabilities for intrusion and data loss prevention, as well as network traffic analysis and data forensics to effectively respond to computer security incidents on DOI's computer networks. We are currently evaluating DOI's capabilities to detect, report, respond to, and recover from computer security incidents and will issue a report of findings and recommendations in fiscal year 2017.

Data Loss Prevention Capabilities

DOI uses a data loss prevention (DLP) system to identify types of attempted data exfiltration, to include PII and other sensitive data. DLP capabilities are imperative to identify and promptly respond to cyberattacks and prevent the theft (exfiltration) of sensitive data. This toolset can be used to scan computer system hardware assets like computer servers and desktops for the presence of sensitive data. DOI also has tools in place to proactively recognize when a system is being compromised at the start of a typical data exfiltration process and notify incident response staff to take action on the system before data exfiltration activities can be successfully completed. DOI has an additional tool in place to proactively recognize and block malware and other forms of malicious network activity, such as potential command and control traffic, as a way to break up data exfiltration processes before cybercriminals try to send data out of the network. Further, DOI utilizes Internet-content filtering tools that block access to known command and control and data dump sites, and email filtering to filter out spam and malicious email-based traffic. Across DOI's desktops, laptops, and servers, an antivirus/malware detection solution has been implemented that detects, quarantines, and remediates known malicious software activities.

DOI also has an intrusion detection system (IDS) and an intrusion prevention system (IPS). The IDS recognizes when malicious activities are happening on a system and notifies DOI incident handlers, who may take action to remediate the incident. The IPS monitors network traffic to detect and prevent vulnerability exploits and flags these activities for DOI to take action.

DOI is also implementing more tools to help prevent the loss of data. One such tool will be a whitelisting solution that will only allow known and approved software packages and updates to run on DOI systems so that

downloaded malware typically used by attackers to steal data will be blocked. In addition, DOI will implement a solution that can flag, test, and block email messages containing potentially malicious content before such spearphishing attacks even get to employee email inboxes.

Forensic and Visibility Capabilities

Data forensics and traffic analysis capabilities are used to dissect security incidents to determine the scope of the incident and its root cause. DOI uses a full-packet capture solution that can be used to investigate security incidents on DOI's network. Forensic tools are used to gather, analyze, and preserve evidence without further compromising the integrity of the already infected system.

DOI plans to implement additional forensic and visibility capabilities. Currently, DOI cannot analyze encrypted traffic. DOI plans to install a decryption device that will provide visibility into encrypted traffic to inspect it for malicious content. Capabilities to analyze encrypted traffic are essential to detect malicious content or data exfiltration that often occurs over encrypted channels. This capability is especially critical because 40 percent of DOI's Internet-bound network traffic is encrypted. DOI also plans to implement an enterprise-level Security Information and Event Management (SIEM) solution that provides centralized, real-time analysis of security alerts generated by network hardware and applications, as well as centralized log management. A SIEM provides capabilities to correlate information technology security incidents from multiple sources on DOI's network to effectively identify the extent of security incidents and coordinate incident response.

Digital Rights Management Capabilities

DOI stated that it does not have specific requirements for Digital Rights Management (DRM) because Federal regulations do not require DRM. DRM refers to the use of protection mechanisms in files to prevent the unauthorized alteration or disclosure of sensitive data. For example, DRM can be used to secure files so that only intended users can authenticate and view the content, define what the user is actually able to do with files like printing or copying, provide version tracking, set expiration dates after which the file cannot be opened, and continuously monitor activity to determine whether someone is using files inappropriately. DOI does have DRM capabilities on documents that are stored in Google Drive, including preventing document editors from changing access and adding new users; disabling options to download, print, and copy; and configuration of document expiration timelines. These DRM options, however, are not available for documents housed on DOI's systems outside of the Google environment (e.g., Microsoft Office or Adobe PDF). According to the OCIO, DOI submitted requests for resources to implement DRM capabilities in the fiscal year 2017 budget, but the request was not approved. Inadequate DRM capabilities could result in the unauthorized alteration or disclosure of sensitive data.

Management of Contractor Systems

In September 2013, OCIO issued a memorandum requiring that all contractor systems follow the same security requirements as computer systems operated by DOI. DOI requires contractors to implement NIST-required security controls prescribed by security categorization of the computer system. Computer systems containing PII are categorized as moderate impact, so the contractor is required to implement the minimum security controls for moderate-impact systems. DOI requires contractors to run DOI-specific system traffic through a DOI-monitored network connection so that DOI's threat monitoring, forensic capabilities, and DLP tools can be used on that traffic. Ensuring that contractor systems implement the appropriate security controls reduces the risk of unauthorized access and disclosure of DOI data in computer systems operated by Federal contractors.

Conclusion

DOI has implemented measures, such as multifactor authentication to reduce the risk of unauthorized access to its covered systems, and software inventory management to comply with intellectual property rights and prevent spending public funds on unused software. DOI, however, needs to update its logical access controls to meet current NIST standards to ensure that general users do not have access to privileged functions and that audit trails are in place to monitor actions taken by privileged users to mitigate risks from insider threats. DOI also needs to ensure that its mobile computing devices are encrypted and securely configured to prevent the loss of sensitive data when these devices are lost or stolen. Finally, DOI needs the ability to inspect encrypted traffic for malicious content to prevent the loss of sensitive data.

Appendix 1: Scope and Methodology

Scope

To accomplish our objective, we reviewed the U.S. Department of the Interior's (DOI's) security policies, procedures, and practices for logical access control policies and practices, use of multifactor authentication, software inventory, threat prevention, and contractor oversight for systems that contain personally identifiable information (PII). We conducted our inspection from February 2016 to July 2016. Our report does not contain any recommendations because Section 406 of the Cybersecurity Act of 2015 only requires us to report on DOI's current conditions.

Methodology

At the time of our inspection, DOI reported that it operated 88 covered systems—72 DOI computer systems, and 16 contractor computer systems—that provide access to PII. As of March 31, 2016, DOI reported 71,290 general and 4,728 privileged users of its computer systems.

We sampled DOI systems that contain PII and reviewed system documentation for access controls. We reviewed security documentation for 10 percent of DOI's 88 computer systems that contain PII (7 DOI systems and 2 contractor systems). We compared the logical access controls in the security documentation for the selected systems with the corresponding minimum logical access controls required by National Institute of Standards and Technology Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," implemented in April 2013, for a moderate-impact computer system. We also interviewed information technology employees responsible for implementing security controls on DOI computer networks and covered systems. Our review included all DOI bureaus and offices and was limited to covered systems.[1]

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

[1] Our review did not include the general support system operated by our office, which contains personally identifiable information.

Appendix 2: Minimum Logical Access Controls for Moderate Impact System

The National Institute of Standards and Technology (NIST) requires minimum logical access controls for a moderate-impact Federal computer system to help ensure the availability of the computer system, as well as the confidentiality and integrity of the sensitive data it contains.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

The organization—

a. develops, documents, and disseminates to organization-defined personnel or roles:
    1. an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. procedures to facilitate the implementation of the access control policy and associated access controls;
b. reviews and updates the current—
    1. access control policy; and
    2. access control procedures.

AC-2 ACCOUNT MANAGEMENT

The organization—

a. identifies and selects types of information system accounts to support organizational missions and business functions;
b. assigns account managers for information system accounts;
c. establishes conditions for group and role membership;
d. specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. requires approvals by organization-defined personnel or roles for requests to create information system accounts;
f. creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
g. monitors the use of information system accounts;
h. notifies account managers—
    1. when accounts are no longer required;
    2. when users are terminated or transferred; and
    3. when individual information system usage or need-to-know changes;
i. authorizes access to the information system based on—
    1. a valid access authorization;
    2. intended system usage; and

3. other attributes as required by the organization or associated missions and business functions;

j. reviews accounts for compliance with account management requirements; and

k. establishes a process for reissuing shared or group account credentials (if deployed) when individuals are removed from the group.

AC-2(1) ACCOUNT MANAGEMENT – *Automated System Account Management*

The organization employs automated mechanisms to support the management of information system accounts.

AC-2(2) ACCOUNT MANAGEMENT – *Removal of Temporary and Emergency Accounts*

The information system automatically removes or disables temporary and emergency accounts after an organization-defined time period for each type of account.

AC-2(3) ACCOUNT MANAGEMENT – *Disable Inactive Accounts*

The information system automatically disables inactive accounts after organization-defined time period.

AC-2(4) ACCOUNT MANAGEMENT – *Automated Audit Actions*

The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies organization-defined personnel or roles.

AC-3 ACCESS ENFORCEMENT

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-4 INFORMATION FLOW ENFORCEMENT

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.

AC-5 SEPARATION OF DUTIES

The organization—

a. separates organization-defined duties of individuals;

b. documents separation of duties of individuals; and

c. defines information system access authorizations to support separation of duties.

AC-6 LEAST PRIVLEGE
The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-6(1) LEAST PRIVLEGE – *Authorize Access to Security Functions*
The organization explicitly authorizes access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.

AC-6(2) LEAST PRIVILEGE – *Nonprivileged Access for Nonsecurity Functions*
The organization requires that users of information system accounts or roles with access to organization-defined security functions or security-relevant information use nonprivileged accounts or roles, when accessing nonsecurity functions.

AC-6(5) LEAST PRIVILEGE – *Privileged Accounts*
The organization restricts privileged accounts on the information system to organization-defined personnel or rules.

AC-6(9) LEAST PRIVILEGE – *Auditing Use of Privileged Functions*
The information system audits the execution of privileged functions.

AC-6(10) LEAST PRIVILEGE – *Prohibit Nonprivileged Users from Executing Privileged Functions*
The information system prevents nonprivileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards or countermeasures.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
The information system—

a. enforces a limit of organization-defined number of consecutive invalid logon attempts by a user during an organization-defined time period; and
b. automatically locks the account or node for an organization-defined time period; locks the account or node until released by an administrator; delays next logon prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

The information system—

a. displays to users an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that—
    1. users are accessing a U.S. Government information system;
    2. information system usage may be monitored, recorded, and subject to audit;
    3. unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
    4. use of the information system indicates consent to monitoring and recording;
b. retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to logon to or further access the information system; and
c. for publicly accessible systems—
    1. displays system use information organization-defined conditions, before granting further access;
    2. displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    3. includes a description of the authorized uses of the system.

AC-11 SESSION LOCK

The information system—

a. prevents further access to the system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and
b. retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11(1) SESSION LOCK – *Pattern-Hiding Displays*

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AC-12 SESSION TERMINATION

The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

The organization—

a. identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions; and
b. documents and provides supporting rationale in the security plan for the information system and user actions not requiring identification or authentication.

AC-17 REMOTE ACCESS

The organization—

a. establishes and documents usage restrictions, configuration or connection requirements, and implementation guidance for each type of remote access allowed; and
b. authorizes remote access to the information system prior to allowing such connections.

AC-17(1) REMOTE ACCESS – *Automated Monitoring and Control*

The information system monitors and controls remote access methods.

AC-17(2) REMOTE ACCESS – *Protection of Confidentiality and Integrity Using Encryption*

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(3) REMOTE ACCESS – *Managed Access Control Points*

The information system routes all remote accesses through organization defined number of managed network access control points.

AC-17(4) REMOTE ACCESS – *Privileged Commands Access*

The organization—

a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for organization defined needs; and
b. Documents the rationale for such access in the security plan for the information system.

AC-18 WIRELESS ACCESS

The organization—

a. establishes usage restrictions, configuration and connection requirements, and implementation guidance for wireless access; and
b. authorizes wireless access to the information system prior to allowing such connections.

AC-18(1) WIRELESS ACCESS – *Authentication and Encryption*

The information system protects wireless access to the system using authentication of selection of one or more users or devices and encryption.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

The organization—

a. establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. authorizes the connection of mobile devices to organizational information systems.

AC-19(5) ACCESS CONTROL FOR MOBILE DEVICES – *Full Device Container or Based Encryption*

The organization employs encryption to protect the confidentiality and integrity of information on mobile devices.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, or maintaining external information systems, allowing authorized individuals to—

a. access the information system from external information systems; and
b. process, store, or transmit organization-controlled information using external information systems.

AC-20(1) USE OF EXTERNAL INFORMATION SYSTEMS – *Limits on Authorized Use*

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization—

a. verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
b. retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-20(2) USE OF EXTERNAL INFORMATION SYSTEMS – *Portable Storage Devices*

The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.

AC-21 INFORMATION SHARING

The organization—

a. facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required; and
b. employs organization-defined automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

AC-22 PUBLICLY ACCESSIBLE CONTENT

The organization—

a. designates individuals authorized to post information onto a publicly accessible information system;
b. trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. reviews the content on the publicly accessible information system for nonpublic information organization-defined frequency and removes such information, if discovered.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081
Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240