June 23, 2006

M-06-16

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
                  Deputy Director for Management

SUBJECT: Protection of Sensitive Agency Information

In an effort to properly safeguard our information assets while using information technology, it is essential for all departments and agencies to know their baseline of activities.

The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:

1.   Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2.   Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
3.   Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4.   Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

Most departments and agencies have these measures already in place. We intend to work with the Inspectors General community to review these items as well as the checklist to ensure we are properly safeguarding the information the American taxpayer has entrusted to us. Please ensure these safeguards have been reviewed and are in place within the next 45 days.

Attachment

Security Checklist

Protection of "Remote" Information

This checklist provides specific actions to be taken by federal agencies for the protection of Personally Identifiable Information (PII) categorized in accordance with FIPS 199 as moderate or high impact that is either:

- Accessed remotely; or

- Physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants).

The specific intent is to compensate for the protections offered by the physical security controls when information is removed from, or accessed from outside of the agency location. Additionally, this checklist has been developed from existing guidance with the expectation that information security is a mission requirement essential to achieving the operational benefits of information technology without exposing the agency, its assets, or individuals to undue risk.

The security controls and associated control assessment methods/procedures in this checklist were taken from NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* and NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006.[1] The controls and assessment methods/procedures in the checklist are a subset of what is currently required for moderate and high impact information systems. However, the checklist does include specific guidance on the technology to be used for some controls.

References:

Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006.

---

[1] For purpose of this Security Checklist, the assessment methods and procedures outlined in NIST Special Publication 800-53A (Second Public Draft), dated April 2006, are considered mandatory. Updated control assessment methods and procedures will be effective upon final publication of Special Publication 800-53A.
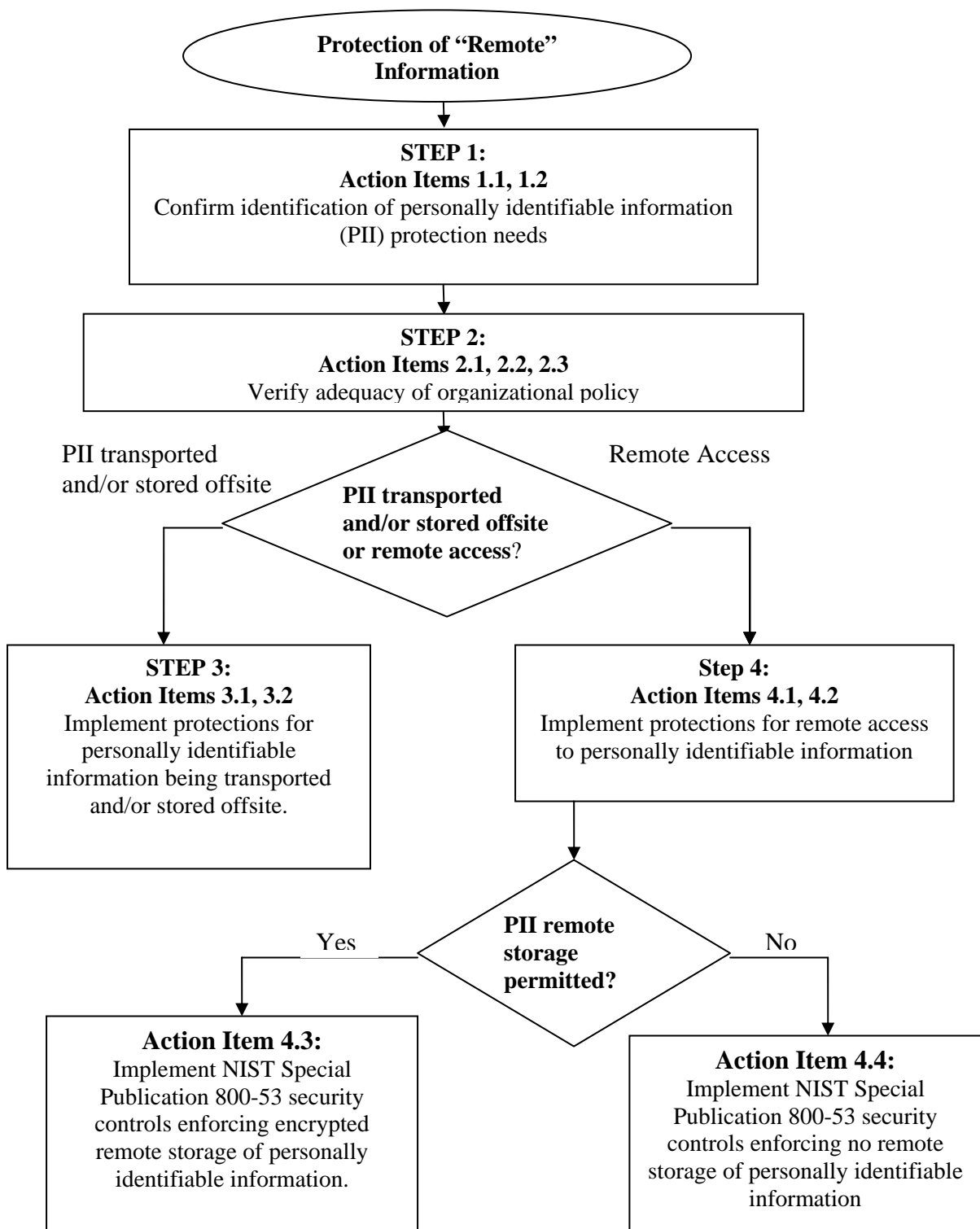
```
                    ╭─────────────────────────╮
                    │  Protection of "Remote"  │
                    │       Information        │
                    ╰─────────────────────────╯
                                 │
                                 ▼
        ┌─────────────────────────────────────────────────────────┐
        │                       STEP 1:                            │
        │                 Action Items 1.1, 1.2                    │
        │  Confirm identification of personally identifiable       │
        │          information (PII) protection needs              │
        └─────────────────────────────────────────────────────────┘
                                 │
                                 ▼
        ┌─────────────────────────────────────────────────────────┐
        │                       STEP 2:                            │
        │               Action Items 2.1, 2.2, 2.3                 │
        │           Verify adequacy of organizational policy       │
        └─────────────────────────────────────────────────────────┘
                                 │
   PII transported                                    Remote Access
   and/or stored offsite         ◇
                              PII transported
                             and/or stored offsite
                             or remote access?
```

STEP 3:
Action Items 3.1, 3.2
Implement protections for personally identifiable information being transported and/or stored offsite.

Step 4:
Action Items 4.1, 4.2
Implement protections for remote access to personally identifiable information

PII remote storage permitted?

Yes

No

Action Item 4.3:
Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information.

Action Item 4.4:
Implement NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information

Figure: Process for Protection of "Remote" Information

	SECURITY CHECKLIST FOR PERSONALLY IDENTIFIABLE INFORMATION THAT IS TO BE TRANSPORTED AND/OR STORED OFFSITE, OR THAT IS TO BE ACCESSED REMOTELY	
	Procedure	
	STEP 1: Confirm identification of personally identifiable information protection needs.	
	Action Item 1.1: Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.	
	Action Item 1.2: Verify existing risk assessment.	
	STEP 2: Verify adequacy of organizational policy.	
	Action Item 2.1: Identify existing organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.	
	Action Item 2.2: Verify that the existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.	
	Action Item 2.3: Revise/develop organizational policy as needed, including steps 3 and 4.	
	If personally identifiable information is to be transported and/or stored offsite, follow Step 3; for remote access to personally identifiable information, follow Step 4.	
	STEP 3: Implement protections for personally identifiable information being transported and/or stored offsite.	
	Action Item 3.1: In those instances where personally identifiable information is transported to a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form.	
	Action Item 3.2: In those instances where personally identifiable information is being stored at a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is stored only in encrypted form.	
	Checklist Complete.	
	STEP 4: Implement protections for remote access to personally identifiable information.	
	Action Item 4.1: Implement NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection.	
	Action Item 4.2: Implement NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information.	
	If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.	
	Action Item 4.3: Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information.	
	Checklist Complete.	
	Action Item 4.4: Implement NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information.	
	Checklist Complete.	

Security Controls and Assessment Procedures

STEP 1: Confirm identification of personally identifiable information protection needs.

Action Item 1.1: Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.

Guidance: The purpose of this step is to review the FIPS 199 security categorization of organizational information with the focus on remote access and physical removal. The intent is to ensure all personally identifiable information through which a moderate or high impact might result has been explicitly identified. For example, databases where the loss, corruption, or unauthorized access to personally identifiable information contained in the databases could result in a serious adverse effect, with widespread impact on individual privacy being one area of specific concern.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

> **PL-5** PRIVACY IMPACT ASSESSMENT
>
> > SP 800-53A: PL-5.1, PL-5.2 (for high impact add: PL-5.3, PL-5.4)
>
> **RA-2** SECURITY CATEGORIZATION
>
> > SP 800-53A: RA-2.1, RA-2.2, RA-2.3 (for high impact add: RA-2.4, RA-2.5)

Action Item 1.2: Verify existing risk assessment.

Guidance: The purpose of this step is to apply the results from the previous action item and operational experience to confirm or modify as needed the existing risk assessment associated with remote access and physical removal of personally identifiable information.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

> **RA-4** RISK ASSESSMENT UPDATE
>
> > SP 800-53A: RA-4.1, RA-4.2, RA-4.3 (for high impact add: RA-4.4, RA-4.5)

STEP 2: Verify adequacy of organizational policy.

Action Item 2.1: Identify existing organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

Guidance: This step is primarily to identify the existing policy related to the security and privacy needs associated with personally identifiable information accessed remotely or physically removed from agency-controlled areas.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

> See action item 2.3.

Action Item 2.2: Verify that the existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

Guidance: Having determined which existing policy is applicable to the remote access or physical removal of personally identifiable information, the purpose of this action item is to verify the adequacy of that policy. The policy should address the following specific questions:

1. For *Personally Identifiable Information* physically removed:

   a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?

   b. For personally identifiable information that can be removed, does the policy require the information be encrypted and that appropriate procedures, training, and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?

2. For *Personally Identifiable Information* accessed remotely:

   a. Does the policy explicitly identify the rules for determining whether remote access is allowed?

   b. When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token?

   c. When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.)

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

See action item 2.3.

Action item 2.3: Revise/develop organizational policy as needed, including steps 3 and 4.

Guidance: Based upon the results from the previous action items, the organizational policy is revised or developed to fully address the questions posed in the previous action items.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-1   ACCESS CONTROL POLICY AND PROCEDURES

      SP 800-53A: AC-1.1, AC-1.2, AC-1.3, AC-1.4 (for high impact add: AC-1.5, AC-1.6, AC-1.7)

AT-1   SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

      SP 800-53A: AT-1.1, AT-1.2, AT-1.3, AT-1.4 (for high impact add: AT-1.5, AT-1.6, AT-1.7)

AU-1   AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

> SP 800-53A: AU-1.1, AU-1.2, AU-1.3, AU-1.4 (for high impact add: AU-1.5, AU-1.6, AU-1.7)

IA-1   IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

> SP 800-53A: IA-1.1, IA-1.2, IA-1.3, IA-1.4 (for high impact add: IA-1.5, IA-1.6, IA-1.7)

MP-1   MEDIA PROTECTION POLICY AND PROCEDURES

> SP 800-53A: MP-1.1, MP-1.2, MP-1.3, MP-1.4 (for high impact add: MP-1.5, MP-1.6, MP-1.7)

SC-1   SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

> SP 800-53A: SC-1.1, SC-1.2, SC-1.3, SC-1.4 (for high impact add: SC-1.5, SC-1.6, SC-1.7)

If personally identifiable information is to be transported and/or stored offsite, follow Step 3; for remote access to personally identifiable information, follow Step 4.

STEP 3: Implement protections for personally identifiable information being transported and/or stored offsite.

Action Item 3.1: In those instances where personally identifiable information is transported to a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form.

Guidance: The intent is to apply the controls necessary to ensure that personally identifiable information is appropriately encrypted prior to being removed from the area under agency control.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

MP-5   MEDIA TRANSPORT

> SP 800-53A: MP-5.1, MP-5.2, MP-5.3 (for high impact add: MP-5.4, MP-5.5)

SC-13   USE OF VALIDATED CRYPTOGRAPHY

> SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

Action Item 3.2: In those instances where personally identifiable information is being stored at a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is stored only in encrypted form.

Guidance: The intent is to apply the controls necessary to ensure that personally identifiable information remains appropriately encrypted during remote storage. This includes establishing and training users on the rules of behavior and information use that will help prevent unencrypted forms of the information from being stored on remote components of the information system.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

PL-4   RULES OF BEHAVIOR

SP 800-53A: PL-4.1, PL-4.2, PL-4.3, PL-4.4, PL-4.5 (for high impact add: PL-4.6, PL-4.7)

SC-4   INFORMATION REMNANTS

SP 800-53A: SC-4.1, SC-4.2 (for high impact add: SC-4.3, SC-4.4)

SC-13   USE OF VALIDATED CRYPTOGRAPHY

SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

STEP 4: Implement protections for remote access to personally identifiable information.

General Guidance: This step is executed when the policy allows remote access to personally identifiable information.

Action Item 4.1: Implement NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection.

Guidance: The intent is to apply those controls necessary to both mandate and achieve connections from remote components of the information system to an internal agency network via a virtual private network (VPN). The VPN is established based upon authentication using agency-controlled certificates or hardware tokens issued directly to each authorized user.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-17   REMOTE ACCESS, with Enhancements (1), (2), and (3)

SP 800-53A: AC-17.1, AC-17.2, AC-17.3, AC-17.4, AC-17.5, AC-17.6, AC-17.7, AC-17.10, AC-17.11, AC-17.13, AC-17.15 (for high impact add: AC-17.8, AC-17.9, AC-17.12, AC-17.14, AC-17.16)

IA-5   AUTHENTICATOR MANAGEMENT

SP 800-53A: IA-5.1, IA-5.2, IA-5.3, IA-5.4, IA-5.5, IA-5.6 (for high impact add: IA-5.7, IA-5.8, IA-5.9)

Action Item 4.2: Implement NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information.

Guidance: This action item is executed when the policy allows personally identifiable information to be downloaded to a remote location. The intent is to apply controls necessary to enable and enforce only appropriate downloading. Included are controls for accessing only allowed information, for least privilege (of downloaded information) necessary to perform duties, for what information is allowed to be transmitted across a remote connection, and for maintaining accountability for actions taken across the remote interface.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-3   ACCESS ENFORCEMENT, with Enhancement (1)

SP 800-53A: AC-3.1, AC-3.2, AC-3.3, AC-3.4, AC-3.7, AC-3.8 (for high impact add: AC-3.5, AC-3.6, AC-3.9)

AC-4   INFORMATION FLOW ENFORCEMENT

SP 800-53A: AC-4.1, AC-4.2, AC-4.3 (for high impact add: AC-4.4, AC-4.5)

AC-6   LEAST PRIVILEGE

SP 800-53A: AC-6.1, AC-6.2, AC-6.3, AC-6.4 (for high impact add: AC-6.5, AC-6.6)

AC-13   SUPERVISION AND REVIEW — ACCESS CONTROL, with Enhancement (1) for high impact information

SP 800-53A: AC-13.1, AC-13.2, AC-13.3, AC-13.4 (for high impact add: AC-13.5, AC-13.6, AC-13.7, AC-13.8, AC-13.9)

AU-2   AUDITABLE EVENTS

SP 800-53A: AU-2.1, AU-2.2, AU-2.3 (for high impact add: AU-2.4, AU-2.5)

AU-6   AUDIT MONITORING, ANALYSIS, AND REPORTING, with Enhancement (1) for high impact information

SP 800-53A: AU-6.1, AU-6.2, AU-6.3 (for high impact add: AU-6.4, AU-6.5, AU-6.6, AU-6.7)

If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.

Action Item 4.3: Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information.

Guidance: This action item is executed when policy allows personally identifiable information to be downloaded to a remote location. The intent is to apply those controls that both mandate and achieve encrypted storage of the information at the remote location.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

PL-4   RULES OF BEHAVIOR

SP 800-53A: PL-4.1, PL-4.2, PL-4.3, PL-4.4, PL-4.5 (for high impact add: PL-4.6, PL-4.7)

SC-4   INFORMATION REMNANTS

SP 800-53A: SC-4.1, SC-4.2 (for high impact add: SC-4.3, SC-4.4)

SC-13   USE OF VALIDATED CRYPTOGRAPHY

SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

Action Item 4.4: Implement NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information.

Guidance: This action item is executed when policy allows personally identifiable information to be remotely accessed only if not stored locally. The intent is to apply

those controls necessary to achieve remote use without local storage. The implementation of these controls will result in only necessary information being transmitted to the remote component of the information system. An example is transaction-based database access that provides no more information to the remote information system component than necessary for the immediate transaction. Another example is allowing downloading of only partial information to mitigate the risk by reducing the potential impact; for example, only extracts/views of a database or only views of statistical information.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-3 ACCESS ENFORCEMENT, with Enhancement (1)

SP 800-53A: AC-3.1, AC-3.2, AC-3.3, AC-3.4, AC-3.7, AC-3.8 (for high impact add: AC-3.5, AC-3.6, AC-3.9)

AC-4 INFORMATION FLOW ENFORCEMENT

SP 800-53A: AC-4.1, AC-4.2, AC-4.3 (for high impact add: AC-4.4, AC-4.5)

AC-6 LEAST PRIVILEGE

SP 800-53A: AC-6.1, AC-6.2, AC-6.3, AC-6.4 (for high impact add: AC-6.5, AC-6.6)

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL, with Enhancement (1) for high impact information

SP 800-53A: AC-13.1, AC-13.2, AC-13.3, AC-13.4 (for high impact add: AC-13.5, AC-13.6, AC-13.7, AC-13.8, AC-13.9)

AC-17 REMOTE ACCESS, with Enhancements (1), (2), and (3)

SP 800-53A: AC-17.1, AC-17.2, AC-17.3, AC-17.4, AC-17.5, AC-17.6, AC-17.7, AC-17.10, AC-17.11, AC-17.13, AC-17.15 (for high impact add: AC-17.8, AC-17.9, AC-17.12, AC-17.14, AC-17.16)

AT-2 SECURITY AWARENESS

SP 800-53A: AT-2.1, AT-2.2, AT-2.3 (for high impact add: AT-2.4, AT-2.5)

AU-2 AUDITABLE EVENTS

SP 800-53A: AU-2.1, AU-2.2, AU-2.3 (for high impact add: AU-2.4, AU-2.5)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING, with Enhancement (1) for high impact information

SP 800-53A: AU-6.1, AU-6.2, AU-6.3 (for high impact add: AU-6.4, AU-6.5, AU-6.6, AU-6.7)

PL-4 RULES OF BEHAVIOR

SP 800-53A: PL-4.1, PL-4.2, PL-4.3, PL-4.4, PL-4.5 (for high impact add: PL-4.6, PL-4.7)

SC-4 INFORMATION REMNANTS
SP 800-53A: SC-4.1, SC-4.2 (for high impact add: SC-4.3, SC.4.4)