UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INSPECTOR GENERAL

THE INSPECTOR GENERAL

October 12, 2006

The Honorable Karen S. Evans
Administrator for Electronic Government and Information Technology
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Ms. Evans:

At your request, the IG community has assessed Departments' and Agencies' status in meeting the requirements of Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Agency Information*.

Offices of Inspectors General (OIG) completed 51 reviews during the period August 7 to September 22, 2006. The results of two reviews are classified and were transmitted to OMB directly by the participating OIG.

On behalf of the President's Council on Integrity & Efficiency (PCIE) and Executive Council on Integrity & Efficiency (ECIE), my office has compiled a consolidated report for the remaining 49 reviews. Please find attached *Federal Agencies' Efforts to Protect Sensitive Information, A Report to the Office of Management and Budget*. We will post this report on the PCIE/ECIE web site, where it will be available to the public.

We are also submitting the individual responses from each PCIE/ECIE member that participated, in two volumes. We consider this agency-specific information sensitive and caution that these volumes should be safeguarded to prevent improper disclosure of the information they contain.

Should you have any questions, please contact Charles Coe, Assistant Inspector General for Information Technology Audits and Computer Crime Investigations. Mr. Coe can be reached at 202-245-7033.

Sincerely,

/S/

John P. Higgins, Jr.
Inspector General, U.S. Department of Education
and Chair, PCIE IT Roundtable

Federal Agencies' Efforts to Protect Sensitive Information

A Report to the Office of Management and Budget

President's Council on Integrity and Efficiency
Executive Council on Integrity and Efficiency

October 2006

Introduction

Objective

The objective of this limited scope review was to assess Departments' and Agencies' (agencies) actions taken to ensure personally identifiable information (PII) and other sensitive information are safeguarded, in accordance with Office of Management and Budget (OMB) Memorandum M-06-16, *Protection of Sensitive Agency Information* (the Memorandum, M-06-16).

Background

The June 23, 2006 Memorandum required agencies to assess their baseline of activities and properly safeguard their information assets while using information technology (IT). The Memorandum identified several steps for agencies to complete within 45 days from its issuance.

I. The Memorandum required agencies to apply a National Institute of Standards and Technology (NIST) checklist for protection of information. The checklist identified multiple Action Steps and Action Items intended to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. The checklist called for agencies to:
   Step 1 – Confirm identification of PII protection needs.
   Step 2 – Verify the adequacy of organizational policy.
   Step 3 – Implement (or verify) protections for PII being transported and/or stored offsite.
   Step 4 – Implement (or verify) protections for remote access to PII.

II. The Memorandum also recommended agencies take the following additional 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 the agency's 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.

OMB requested that the Inspectors General (IG) community help assess the status of these safeguards by reviewing agencies' progress in meeting the Memorandum's requirements. In response to OMB's request, the IG community conducted a limited scope review between August 7 and September 22, 2006. The consolidated results from this review are the subject of this President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) report.

Scope and Methodology

The PCIE/ECIE Federal Audit Executive Council (FAEC) IT Committee was tasked to develop a *Review Guide* and a *Data Collection Instrument* (DCI) to capture the results of the IG community's assessment of agency efforts to protect sensitive information.

Participating IGs were required to use the review guide and DCI to assess and document their agency's compliance with Memorandum requirements. With this guidance, PCIE/ECIE did not stipulate a specific assessment methodology for IGs to follow. Rather, the guidance provided suggested review steps and a standard format to facilitate consolidated government-wide reporting on adherence to the Memorandum. The review guide and DCI were closely linked to the specific actions required with the Memorandum.

To further assist the PCIE IT Roundtable in creating the government-wide response, participating IGs were also asked to specify the type of work completed, and describe the assessment methodology used by providing descriptors generally consistent with NIST Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems.* SP800-53A, Appendix D describes three assessment methods that can be used to help determine whether a particular security control is effective in its application: interviews; examinations; and/or tests. Interviews and examinations can be of generalized, focused, or comprehensive depth; and several types of tests can be conducted (i.e., functional testing, penetration testing, structural testing). IGs were asked to identify the methods used, including depth of interviews or examinations conducted. With respect to tests, IGs were simply asked whether they conducted any tests to independently verify controls.

Offices of Inspector General (OIG) completed 51 reviews. The results from two agencies were submitted directly to OMB, and results from the remaining 49 reviews were aggregated in this consolidated report. Each participating OIG applied professional judgment to determine appropriate methods, tools and type of work to use to complete the suggested review steps detailed in the review guide, and to answer specific questions covered in the DCI. While the methodologies and depth of work varied between OIGs, almost all conducted examinations to validate agency status, and approximately two thirds reported testing one or more areas of review.

Results of Review

Summary Responses

In interpreting the graphs presented in our report, the reader should keep several points in mind:

- When addressing Section I, steps 1 – 4, some OIGs responded to the high-level, summary question posed at the start of each Step, while others left this question blank, exclusively responding to the subset of Action Items. Responses to other questions were occasionally left blank. The bar graphs reflect the responses for which the OIGs provided a response.
- Some OIGs identified a number of questions as "Not Applicable" to their respective agencies. The bar graphs specifically identify the "Not Applicable" responses.
- Responses of "Partial" (or partially) reflect a combination of possible scenarios. For example, an OIG response of partial may reflect an agency that has performed only part of the requirements identified in the Memorandum Step or Action Item. It may also reflect an agency that has performed the Step or Action Item, but only for a portion of its systems or a limited number of organizational subcomponents.
- Within a Step, the number of respondents with a given answer may not represent the same agency. For example, in the graph below, while there are 13 "Yes" answers for each of the three questions, 11 agencies responded "Yes" to all and five agencies responded "Yes" to one or two of the three questions.

Three Quarters of the Agencies Are Still in the Process of Confirming PII Protection Needs

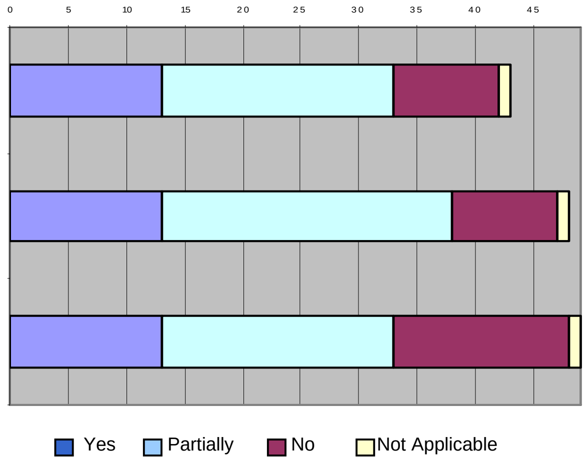
For the 49 responses consolidated here, only 11 OIGs report that their agency has confirmed identification of PII protection needs, including verification of information categorization and existing risk assessments. By and large, agencies are still in the process of verifying information categorization to ensure identification of PII requiring protection when accessed remotely or physically removed; and/or verifying existing risk assessments.

Verification of Need for PII Protection

STEP 1: Has the Agency confirmed identification of personally identifiable information protection needs? If so, to what level?

Action Item 1.1: Has the Agency verified information categorization to ensure identification of personal identifiable information requiring protection when accessed remotely or physically removed?

Action Item 1.2: Has the Agency verified existing risk assessments?



Agencies Have Made Progress in Verifying or Ensuring the Adequacy of Organizational Policy But Much Work Remains

Agencies are making progress in ensuring that their organization policies adequately address the physical removal, remote access, and remote download and storage of sensitive PII information. However, based on individual OIG reports and comments, it is apparent that developing policies that are actionable and enforceable remains a challenge; so is including sufficient details to address many possible scenarios.

Adequacy of Policy

STEP 2: Has the Agency verified the adequacy of organizational policy? If so, to what level?

Action Item 2.1: Has the Agency identified 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: Does the existing Agency organizational policy address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed?

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

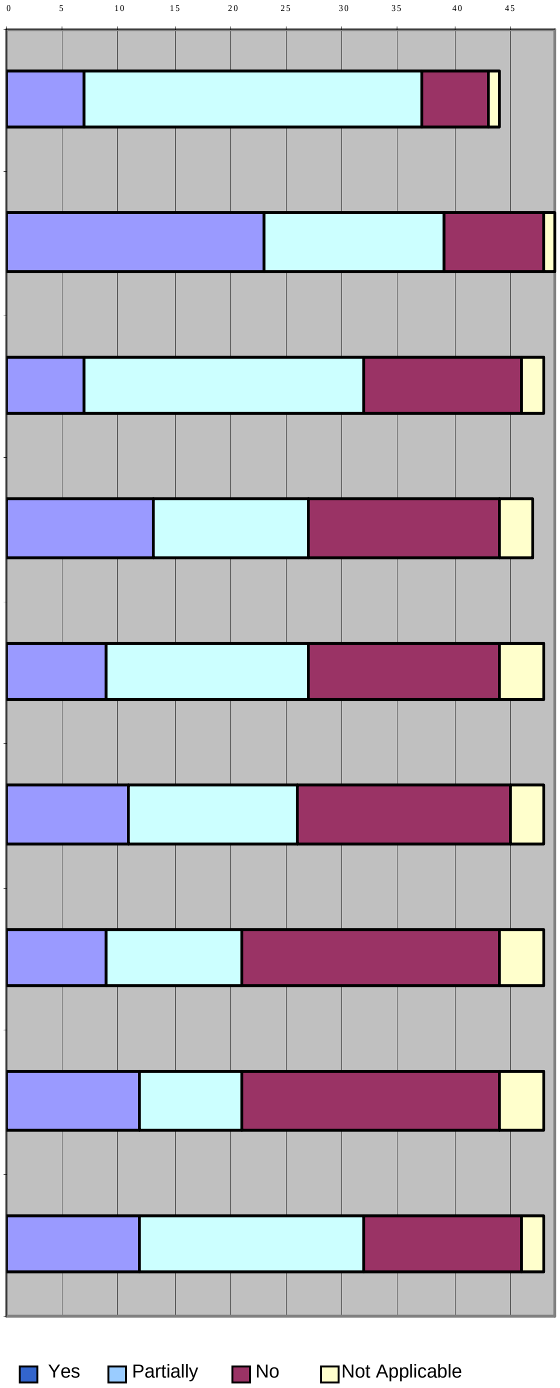
2.2.1.b. For personally identifiable information that can be removed, does the policy require that information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protection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

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

2.2.2.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 tokens?

2.2.2.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.)

Action Item 2.3: Has the organizational policy been revised or developed as needed, including steps 3 and 4?



Implementation Challenges Are Not Insignificant

Individual OIG reports highlight the technical and organizational implementation and enforcement complexities. As agencies take steps to verify that adequate protections are in place for sensitive PII that is transported, or remotely accessed, downloaded and stored, challenges are varied and significant. For example, unless encryption is systematically implemented using solutions that require little user-initiated intervention, enforcement is not fully feasible. Several OIGs report that agencies are exploring comprehensive encryption solutions, and some have plans in place for a FY2007 acquisition. Also, a number of agencies are using risk-based approaches to prioritize the implementation of safeguards

Adequacy of Protections

STEP 3: Has the Agency implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level?

Action Item 3.1: In the instance where personally identifiable information is transported to a remote site, have the NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form been implemented?

Action Item 3.2: In the instance where PII is being stored at a remote site, have the NIST SP 800-53 security controls ensuring that information is stored only in encrypted form been implemented?

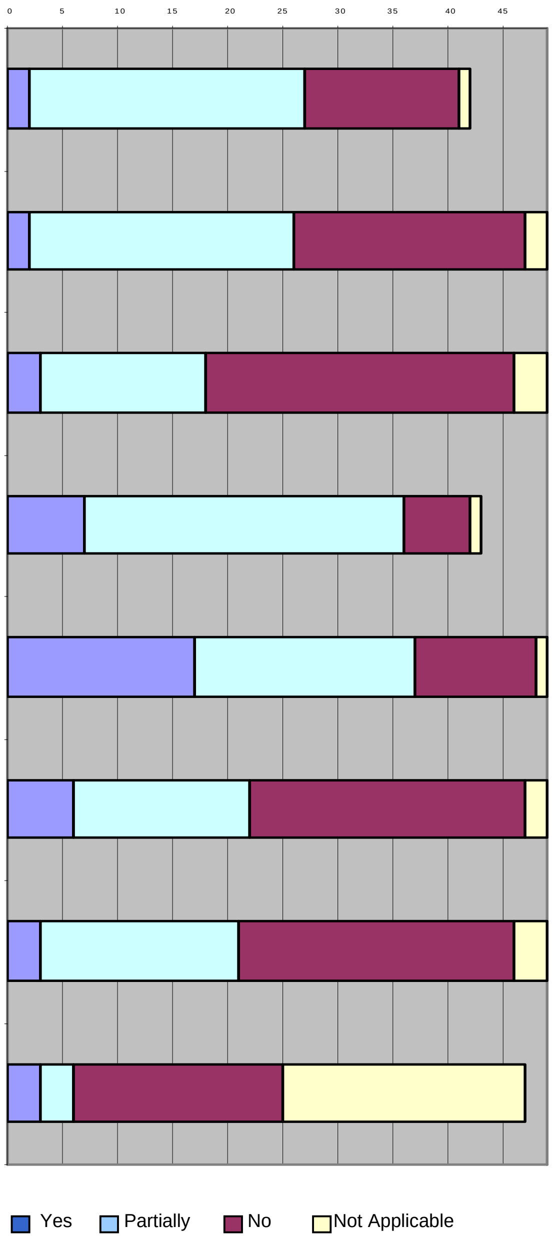
STEP 4: Has the Agency implemented protections for remote access to personally identifiable information? If so, to what level?

Action Item 4.1: Have NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection been implemented by the Agency?

Action Item 4.2: Have the NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information been enforced by the Agency?

Action Item 4.3: Have the NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information been implemented by the Agency?

Action Item 4.4: Has the Agency enforced NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?



Agencies Show Mixed Results on OMB's Request for Additional Actions

While many agencies have implemented "time-out" functions that require re-authentication after a period of inactivity, most agencies do not log all computer-readable extracts from databases holding sensitive information and verify that each such extract has been erased within 90 days unless its use is still required. Continued progress is required with respect to encrypting all sensitive data on mobile computers/devices and implementing two-factor remote access authentication.

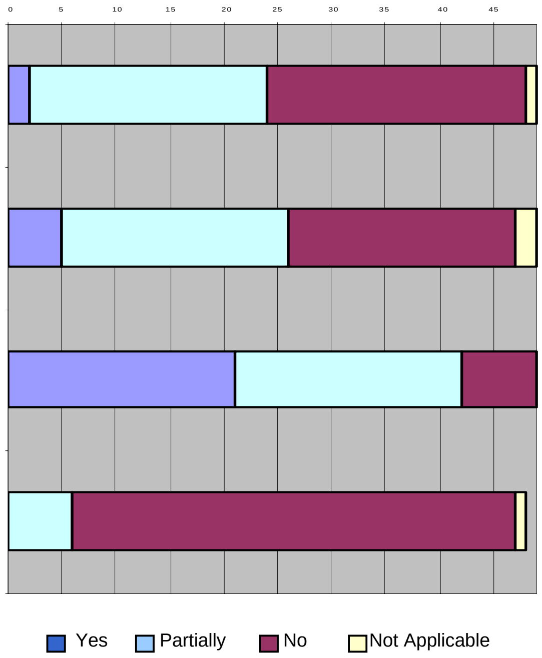
Additional Agency Actions Recommended by M-06-16

1. Has the Agency encrypted all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?

2. Does the Agency use remote access with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access?

3. Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity?

4. Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data has been erased within 90 days or its use is still required?



Conclusion

Most Federal agencies are still at risk for improper access and disclosure of personally identifiable information and other sensitive data, despite continued progress toward the establishment of appropriate safeguards. There is a continued need for agencies to identify and properly categorize sensitive PII information, to refine organizational policy, and to implement comprehensive solutions to protect PII being transported or stored offsite, or remotely accessed.

The complete results of each individual assessment were provided to OMB. Based on the sensitivity of this information, however, agency-specific details are not included in this report.