DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Letter Report:

DHS Chief Information Officer Remediation Plan

Office of Information Technology

OIG-06-11 **November 2005**

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

November 30, 2005

The Honorable Jerry Lewis, Chairman
Committee on Appropriations
U.S. House of Representatives
H-218 Capitol Building
Washington, DC 20515-6015

Dear Chairman Lewis:

This letter provides the results of our review of the Chief Information Officer's (CIO) plan to address the weaknesses in the Department of Homeland Security's (DHS) information security, as directed in the House Report 109-079 – *Department of Homeland Security Appropriations Bill, 2006*. The House report identified four significant challenges that DHS faces in securing its information systems. Specifically, according to the House report, "The Department lacks a complete and accurate inventory of its information systems; has not tested the contingency plans for the majority of its information systems that it knows it has; is below the government-wide average in reviewing contractor operations, … and, has a poor certification and accreditation process that is not performed consistently across the Department." The Committee directed us to review the CIO's plan and report back to the Committee by November 30, 2005, on the thoroughness of the CIO's plan.

RESULTS OF REVIEW

The Department completed actions to address one of the challenges identified by the Committee prior to developing its plan. The Department had developed a complete and accurate inventory of its sensitive but unclassified and collateral classified systems. The responsibility for the inventory of the Department's intelligence systems falls under the purview of the DHS Office of Security. As a result, the CIO has not included these systems in its inventory. During our evaluation of DHS' security program for its intelligence systems, as required by the Federal Information Security Management Act of 2002 (FISMA) for FY2005, we determined that the intelligence systems inventory was complete and accurate.[1]

We reviewed the initial draft of the CIO's remediation plan and provided our detailed assessment to the DHS Chief Information Security Officer (CISO) on October 28, 2005, identifying parts of the plan that were either incomplete or needed additional clarification to address the challenges identified by the Committee. Based on our review of the revised plan (received on November 9, 2005), we believe that the CIO's remediation plan thoroughly addresses one of the

[1] *Evaluation of DHS' Security Program and Practices For Its Intelligence Systems*, dated August 2005 (OIG-05-34).

three remaining challenges and partially addresses the two other challenges identified by the Committee.

The DHS CIO developed a one-year remediation plan, *Fiscal Year 2006 DHS Information Security Certification and Accreditation Remediation Plan*, to address the three remaining challenges identified in the Committee's report, including the Department's goal of 100% certification and accreditation of all information technology systems. According to the CIO, the remediation plan was not intended to address all of the Department's security weaknesses. Accordingly, we limited our evaluation of the plan to only the challenges identified by the Committee.

The remediation plan thoroughly addresses the challenge of a poor certification and accreditation process. Specifically, under the plan, the CIO developed a certification and accreditation process that can be performed consistently across the Department and enforced by the CIO. The plan, if fully implemented by all DHS' components and the CISO, should give the CIO assurance that all of its non-intelligence systems that have been identified as having a quality certification and accreditation package, have in fact met all of the documentation and testing required to accredit a system.

However, the plan does not completely address two challenges identified by the Committee. The plan will only ensure that by September 30, 2006, all systems that have been accredited have a tested contingency plan as part of its certification and accreditation, and all that contractor-operated systems have been reviewed at least once as part of the certification and accreditation process. In addition, the plan does not address the identified weaknesses of testing contingency plans on a periodic basis, or performing annual reviews of contractor operated systems, as required by the Office of Management and Budget. Further, the plan does not address weaknesses in the information security of the Department's intelligence systems including contingency plan testing and certification and accreditation. While it is noted in the plan that these systems are not under the purview of the CIO, the Committee report did not specifically exclude intelligence systems from its request. The CISO believes, however, that the plan specifically addresses all the challenges identified by the Committee, including those that we believe were only partially addressed.

DISCUSSION WITH MANAGEMENT AND FOLLOW-UP

We discussed the results of this review with the DHS CISO on November 14, 2005, who acknowledged that the plan as originally drafted, needed improvement. The CISO incorporated many of our comments in the updated version of the remediation plan. For the issues described above regarding the periodic testing of contingency plans, annual reviews of contractor operated systems, and weaknesses in the information security of the Department's intelligence systems, we will continue to work with the CIO, and also through our annual evaluation of the Department's security programs, as required by FISMA, to address these challenges.

Should you have questions concerning this report, please call me, or your staff may call Frank Deffer, Assistant Inspector General for Information Technology, at (202) 254-4100.

Sincerely,

Richard L. Skinner

Richard L. Skinner
Inspector General

cc: The Honorable David Obey
Mr. Scott Charbo, DHS Chief Information Officer

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

November 30, 2005

The Honorable David Obey
Committee on Appropriations
U.S. House of Representatives
1016 Longworth Building
Washington, DC 20515-6015

Dear Congressman Obey:

This letter provides the results of our review of the Chief Information Officer's (CIO) plan to address the weaknesses in the Department of Homeland Security's (DHS) information security, as directed in the House Report 109-079 – *Department of Homeland Security Appropriations Bill, 2006*. The House report identified four significant challenges that DHS faces in securing its information systems. Specifically, according to the House report, "The Department lacks a complete and accurate inventory of its information systems; has not tested the contingency plans for the majority of its information systems that it knows it has; is below the government-wide average in reviewing contractor operations, … and, has a poor certification and accreditation process that is not performed consistently across the Department." The Committee directed us to review the CIO's plan and report back to the Committee by November 30, 2005, on the thoroughness of the CIO's plan.

RESULTS OF REVIEW

The Department completed actions to address one of the challenges identified by the Committee prior to developing its plan. The Department had developed a complete and accurate inventory of its sensitive but unclassified and collateral classified systems. The responsibility for the inventory of the Department's intelligence systems falls under the purview of the DHS Office of Security. As a result, the CIO has not included these systems in its inventory. During our evaluation of DHS' security program for its intelligence systems, as required by the Federal Information Security Management Act of 2002 (FISMA) for FY2005, we determined that the intelligence systems inventory was complete and accurate.[1]

We reviewed the initial draft of the CIO's remediation plan and provided our detailed assessment to the DHS Chief Information Security Officer (CISO) on October 28, 2005, identifying parts of the plan that were either incomplete or needed additional clarification to address the challenges identified by the Committee. Based on our review of the revised plan (received on November 9, 2005), we believe that the CIO's remediation plan thoroughly addresses one of the

[1] *Evaluation of DHS' Security Program and Practices For Its Intelligence Systems*, dated August 2005 (OIG-05-34).

three remaining challenges and partially addresses the two other challenges identified by the Committee.

The DHS CIO developed a one-year remediation plan, *Fiscal Year 2006 DHS Information Security Certification and Accreditation Remediation Plan*, to address the three remaining challenges identified in the Committee's report, including the Department's goal of 100% certification and accreditation of all information technology systems. According to the CIO, the remediation plan was not intended to address all of the Department's security weaknesses. Accordingly, we limited our evaluation of the plan to only the challenges identified by the Committee.

The remediation plan thoroughly addresses the challenge of a poor certification and accreditation process. Specifically, under the plan, the CIO developed a certification and accreditation process that can be performed consistently across the Department and enforced by the CIO. The plan, if fully implemented by all DHS' components and the CISO, should give the CIO assurance that all of its non-intelligence systems that have been identified as having a quality certification and accreditation package, have in fact met all of the documentation and testing required to accredit a system.

However, the plan does not completely address two challenges identified by the Committee. The plan will only ensure that by September 30, 2006, all systems that have been accredited have a tested contingency plan as part of its certification and accreditation, and all that contractor-operated systems have been reviewed at least once as part of the certification and accreditation process. In addition, the plan does not address the identified weaknesses of testing contingency plans on a periodic basis, or performing annual reviews of contractor operated systems, as required by the Office of Management and Budget. Further, the plan does not address weaknesses in the information security of the Department's intelligence systems including contingency plan testing and certification and accreditation. While it is noted in the plan that these systems are not under the purview of the CIO, the Committee report did not specifically exclude intelligence systems from its request. The CISO believes, however, that the plan specifically addresses all the challenges identified by the Committee, including those that we believe were only partially addressed.

DISCUSSION WITH MANAGEMENT AND FOLLOW-UP

We discussed the results of this review with the DHS CISO on November 14, 2005, who acknowledged that the plan as originally drafted, needed improvement. The CISO incorporated many of our comments in the updated version of the remediation plan. For the issues described above regarding the periodic testing of contingency plans, annual reviews of contractor operated systems, and weaknesses in the information security of the Department's intelligence systems, we will continue to work with the CIO, and also through our annual evaluation of the Department's security programs, as required by FISMA, to address these challenges.

Should you have questions concerning this report, please call me, or your staff may call Frank Deffer, Assistant Inspector General for Information Technology, at (202) 254-4100.

Sincerely,

Richard L. Skinner

Richard L. Skinner
Inspector General

cc: The Honorable Jerry Lewis
Mr. Scott Charbo, DHS Chief Information Officer

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.