BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 30, 2007

The Honorable Scott Charbo
Chief Information Officer
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Charbo:

The House Committee on Homeland Security is currently conducting a review of federal information system security. The Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held a hearing on April 19, 2007 at which time it was revealed that networks at the Departments of Commerce and State were hacked in 2006. These incidents jeopardize the integrity of our government's information. We are concerned that similar incidents may be occurring within the networks of the Department of Homeland Security. Please provide answers to the following questions:

1. What responsibility does the Chief Information Officer have over the networks of the Department of Homeland Security? Please explain your relationship to the Chief Information Security Officer, as well as the Chief Information Officers and Chief Information Security Officers of the Department's component agencies.

2. Please provide the Department's information security policy and incident response plan.

3. Please provide a report on how many and what types of incidents have been reported to US-CERT by agencies within the Department of Homeland Security. Please categorize each incident using the "Federal Agency Incident and Event Categories" developed by the US-CERT. Please provide details of the attack or attacks during 2004-2007 that were the most critical (classified "CAT 1" on the US-CERT reporting guidelines). Please include both those that were and were not reported to US-CERT, and indicate which were not reported to US-CERT within the US-CERT reporting timeframe.

4. Has the Department taken an inventory of each access point to its network (e.g., every connected device, wireless device, remote device, etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability? Does a complete network topology diagram exist? If so, please provide that diagram.

5. Has the Department ever conducted both internal and external penetration tests on its systems? Have individual components of the Department ever performed internal and external penetration tests on their systems? Please provide copies of all penetration testing reports and narratives describing the vulnerabilities that were revealed and how those vulnerabilities were mitigated.

6. When was the last time the Department used ingress and egress filtering on client personal computers? When was the last time the Department replicated client-side attacks on those computers? Has the Department ever conducted a network-wide rogue tunnel audit of all client personal computers? Have you ever conducted audits on the aforementioned compromised personal computers from question 3?

7. Has the Department implemented a secure coding initiative? What portion of software deployed by the Department and its components have been tested using source code analysis tools? What portion of web applications have been tested using web application security tools? How many of the programmers working on Department applications, whether Department or contractor employees, have been trained in secure coding techniques and what skills testing was undertaken to ensure they had mastered secure coding techniques?

8. Has the Department mandated two-factor authentication for all privileged personnel and system administrators? If not, why not?

9. What legal requirements are the Department's hosting companies, data warehouses, software developers, or application service providers contractually obligated to fulfill regarding security? Please provide a narrative of the duties, layers of security, notification of security breaches, and timeliness of responses that the Department requires of these contractors. Is the Department able to audit/penetration test these entities to ensure that that standard of security has been met? Has the Department ever done so?

10. Please provide the annual budgets for the Chief Information Security Officer beginning in fiscal year 2003.

11. How much money, in total, has the Department spent on meeting the requirements of the Federal Information Security Management Act (FISMA)? What percentage of the overall budget does that figure represent? Specifically, how did those reports lead to improved defenses against attacks? What specific changes were made? Are you confident those changes improved your defenses?

12. When the Department purchases software, do procurement documents require that the purchased software operates effectively on the secure configurations? If not, what does the Department do when a purchased package requires security configurations to be weakened in order to run the purchased application?

13. What are your top three initiatives for securing the Department for 2008? How do you measure those goals?

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, we request a response in writing by not later than May 21, 2007. If you have any questions, please contact, Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security at (202) 226-2616.

Sincerely,

Bennie G. Thompson
Chairman

Peter T. King
Ranking Member

James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, Science and
Technology

Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats,
Cybersecurity, Science and
Technology

Christopher P. Carney
Chairman
Subcommittee on Management,
Investigations, and Oversight

Mike Rogers
Ranking Member
Subcommittee on Management,
Investigations, and Oversight

BGT/jso

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

Homeland Security

MAY 2 1 2007

05-22-07P04:24 RCVD

The Honorable Bennie G. Thompson
Chairman
U.S. House of Representatives Committee on Homeland Security
Washington, DC 20515

Re: Department Information Technology Security Policies and Procedures

Dear Chairman Thompson,

It is my pleasure to provide the following responses to your committee's April 30, 2007 request for information concerning the Department of Homeland Security's (DHS) information technology security policies and procedures. (Attachment 1)

1. **What responsibility does the Chief Information Officer have over networks of the Department of Homeland Security? Please explain your relationship to the Chief Information Security Officer, as well as the Chief Information Officers and Chief Information Security Officers of the Department's component agencies.**

The Department's Chief Information Officer exercises all statutory authorities and Federal mandates assigned to Federal Chief Information Officers, particularly those outlined in the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act of 2002 (FISMA). In accordance with FISMA, the Chief Information Security Officer (CISO) is a direct-report to the Chief Information Officer.

Department of Homeland Security Management Directive 007.1, *Information Technology Integration and Management*, included as Attachment 2, further strengthens the role of the DHS Chief Information Officer in three key areas:

- Review and approval authority over all information technology (IT) purchase requests greater than $2.5 million
- Approval over all Component Chief Information Officer hirings
- Input into Component-level Chief Information Officer performance plans and evaluations.

Component Security Programs are under the direction of Component-level Information Systems Security Managers (ISSMs), who report directly to each of their respective Component Chief Information Officers. ISSMs are required to follow guidance from the Department CISO. Additionally, ISSMs collectively comprise the Information Systems Security Board (ISSB), which is chaired by the Department CISO.

2. **Please provide the Department's information security policy and incident response plan.**

DHS Sensitive Systems Policy Directive 4300A, Version 5.1 and Attachment F – *Incident Response and Reporting* are included as Attachments 3 and 4. These documents represent the Department's current information technology security policy and incident response plan.

3. **Please provide a report on how many and what types of incidents have been reported to US-CERT by agencies within the department of homeland Security. Please categorize each incident using the "Federal Agency Incident and Event Categories" developed by the US-CERT. Please provide details of the attacks during 2004-2007 that were the most critical (classified "CAT 1" on the US-CERT reporting guidelines). Please include both those that were and were not reported to US-CERT, and indicate which were not reported to US-CERT within the US-CERT reporting timeframe.**

Individual DHS Components do not report incidents directly to the US-CERT. The Department has its own 24x7 Security Operations Center (DHS SOC) that oversees all IT security operations for the Department. The DHS SOC has direct operational oversight over of all aspects of the Department's common wide area network (OneNet), and also oversees the vulnerability management and incident reporting processes. Individual Components have security operations capabilities for their own local environments; however, all of these are operationally subordinate to the DHS SOC.

The DHS SOC, and only the DHS SOC, reports incidents to the US-CERT in accordance with US-CERT categorizations and guidelines and in the same manner as the other civilian Federal agencies. Attachment 5 contains a summary report for all incidents reported by the DHS SOC to the US-CERT from October 2004 to the present. The *DHS SOC Security Operations Concept of Operations (CONOPS)* is provided as Attachment 6.

4. **Has the Department taken an inventory of each access point to its network (i.e. every connected device, wireless device, remote device, etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability? Does a complete network topology diagram exist? If so, please provide that diagram.**

The network topology diagrams are provided as Attachments 7a and 7b.

5. **Has the Department ever conducted both internal and external penetration tests on its systems? Have individual Components of the Department ever performed internal and external penetration tests on their systems? Please provide copies of all penetration testing reports and narratives describing the vulnerabilities that were revealed and how those vulnerabilities were mitigated.**

Current DHS Policy requires all Components to conduct annual vulnerability assessments and/or testing to identify security vulnerabilities on IT systems containing sensitive information. Assessments are also required whenever significant system changes are made. The DHS Computer Incident Response Center (CSIRC), an element of the DHS Security Operations Center (SOC), centrally manages the program, which is executed at the Component level. The

CSIRC's role is fully outlined in the SOC CONOPS document (Attachment 5) and is supported within *DHS Sensitive Systems Policy Directive 4300A*[1] (Attachment 2).

DHS Components have implemented internal and external penetration testing programs and currently test all FIPS 199 "high" category systems. General support systems or major applications created or built to meet unique mission needs, receive a full internal penetration test prior to obtaining "Authority to Operate" (ATO). In addition, the DHS Office of the Inspector General (OIG) conducts annual FISMA audits, which include internal penetration testing. Some systems receive periodic manual and automated internal penetration testing. Security Test and Evaluation (ST&E) results, Security Assessment Reports also reveal vulnerabilities. Mitigation actions are uploaded and tracked within the DHS Trusted Agent FISMA (TAF) tool.

Vulnerabilities that can not be mitigated quickly are recorded and tracked within the TAF Plan of Action and Milestone (POA&M) folder. Each POA&M item is assigned a scheduled completion date, lists the vulnerability, and articulates how it will be corrected or mitigated.

Attachment 8 provides a representative sample of the Department's penetration testing activities. The aggregate of additional information would reach a National Security classification level. Should you require additional information, please advise and the Department will arrange for courier delivery of information at the appropriate classification.

6. **When was the last time the Department used ingress and egress filtering on client personal computers? When was the last time the Department replicated client-side attacks on those computers? Has the Department ever conducted a network-wide rogue tunnel audit of all client personal computers? Have you ever conducted audits on the aforementioned compromised personal computers from question 3?**

DHS does not currently apply ingress and egress filtering on individual client personal computers, however all DHS content to and from the Internet is controlled through dedicated gateways and ingress and egress filtering is enforced at those control points.

The DHS approach is similar to that employed by the Department of Defense (DoD) on its Non-classified Internet Protocol Router Network (NIPRNet), where most of the ingress/egress filtering is done at Internet/NIPRNet gateways. The DoD is conducting a pilot program whereby enterprise-wide client side ingress and egress filtering is currently being tested. DHS will review the results from the pilot and determine the best way forward.

DHS has not replicated client-side attacks or rogue tunnel audits on client PCs, however it routinely conducts audits on compromised personal computers. A representative sample of incidents that have been audited and describes the actions taken as a result of compromised systems is provided in Attachment 9.

7. **Has the Department implemented a secure coding initiative? What portion of software deployed by the Department and its components have been tested using source code analysis tools? What portion of web applications have been tested using web application security tools? How many programmers working on Department**

[1] Sections 5.4.2 Network Security Monitoring; 5.4.8 Testing and Vulnerability Management

applications, whether Department or contractor employees, have been trained in secure coding techniques and what skills testing was undertaken to ensure they had mastered secure coding techniques?

The Department of Homeland Security relies heavily on Commercial Off-the-Shelf (COTS) systems and applications. For this reason, Department policy requires that acquisition priority be given to products certified through any one of the three following certification programs:

- The National Security Agency/National Institute of Standards and Technology, National Information Assurance Partnership Evaluation and Validation Program
- International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement
- The National Institute of Standards and Technology (NIST) Federal Information Processing Standards Validation Program

While there is currently no Department-wide secure coding initiative, this practice is addressed in a number of ways.

The DHS Common Operating Environment primarily uses Microsoft software. In FY06/07, the Department supported the Service Oriented Architecture through the use of the Microsoft .NET environment. This coding environment provides a means to produce code to protect against buffer overflows and other threat vectors that could be used to gain privileged access to computing environments.

The Federal Law Enforcement Training Center (FLETC) has limited legacy software applications and associated coding. Although the center has not used secure coding in the past, its latest application, Student Administration and Scheduling System (SASS), currently being developed under contract will be tested using source code analysis tools in the 3rd Quarter of FY07.

The Transportation Security Administration (TSA) is in phase one of implementing source code analysis tools, which it intends to employ on all applications, including web-enabled systems. Implementation will include appropriate training for TSA employees and contract language requiring training for contractor personnel.

Other Components, such as the National Protection and Programs Directorate (NPPD) manually check secure coding against the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) and with the .NET questionnaire. These checklists enable NPPD to ensure that coding is "hardened" in accordance with DHS IT Security Policy.[2]

The United States Citizenship and Immigration Services (USCIS) tests selected enterprise applications as part of an independent validation and verification (IV&V) process. New application code is run through a security test and evaluation (ST&E) process as part of the normal IT lifecycle management methodology.

[2] Hardening in this context means the use of security configuration checklists to greatly improve overall levels of security in organizational systems; however, no checklist can permit a system or a product to become 100 % secure.

Components who do not perform their own source code analysis are required to utilize applications and operating systems found in the DHS Technical Reference Model (TRM) database. The Customs and Border Protection (CBP) Technical Review Committee (TRC), reviews and approves software and hardware for insertion into the TRM. The TRC considers other test results, such as those conducted as part of the National Information Assurance Partnership (NIAP) testing program.

8. **Has the Department mandated two-factor authentication for all privileged personnel and system administrators? If not, why not?**

The Department currently employs a number of two-factor authentication technologies, including the Common Access Card (CAC) and RSA SecureID (Token-based). These technologies were implemented at the Component level and were selected to meet specific mission needs. There is currently no Department-wide solution in place, however two-factor authentication will be incorporated as part of the Department's implementation of Homeland Security Presidential Directive #12 (HSPD-12). HSPD-12 is provided in Attachment 10.

The Department's intent is to move to HSPD-12 compliant PIV cards as rapidly as possible. Cards will be required for all employees, as well as any other individual requiring access to Department's IT resources.

9. **What legal requirements are the Department's hosting companies, data warehouses, software developers, or application service providers contractually obligated to fulfill regarding security? Please provide a narrative of the duties, layers of security, notification of security breaches, and timeliness of responses that the Department requires of these contractors. Is the Department able to audit/ penetration test these entities to ensure that that standard of security has been met? Has the Department ever done so?**

The Department currently operates and maintains a total of 723 production systems:

506 Agency Systems
217 Contractor Systems
723 Total Systems

In addition to complying with all Federal Acquisition Regulations, the Department has published specific Homeland Security Acquisition Regulations (HSAR), in accordance with rule making authority granted when the Department was created. Contractor systems are tracked and maintained within the DHS tracking system and subject to the same rules and requirements as Government systems. The relevant sections and specific language associated with information security activities in the HSAR are included in Attachment 11.

For example, the Inspector General (IG) routinely reviews a sub-set of contractor systems as part of the annual FISMA review. The review includes test results of system controls, conducted as part of the system's Certification and Accreditation (C&A) or required annual test. In addition, the IG has conducted several audits where the information systems were owned and/or managed/operated by contractors (including other Federal agencies) and where system tests were

performed to evaluate the effectiveness of system controls. In developing its FY08 annual performance plan, the IG has identified additional audits that will test and evaluate controls on systems owned and/or managed on behalf of the Department by outside contractors and/or other Federal agencies.

10. Please provide the annual budgets for the Chief Information Security Officer beginning in fiscal year 2003.

2003	Department created (no budget existed for this year)
2004	$12.5M
2005	$17.5M
2006	$15M
2007	$15M

11. How much money, in total, has the Department spent on meeting the requirements of the Federal Information Security Management Act (FISMA)? What percentage of the overall budget does that figure represent? Specifically, how did those reports lead to improved defenses against attacks? What specific changes were made? Are you confident those changes improved your defenses?

Total spending in DHS for IT security is as follows (all dollar figures are in millions):

Year	IT Security	IT Total	IT Security as % of all IT
2006	$312.3	$3811.5	8.2%
2007	$331.7	$4879.6	6.8%

DHS has implemented the Federal Information Security Management Act (FISMA) through a comprehensive set of Department-specific policies that incorporate all federal guidance, including National Institute of Standards and Technology (NIST) standards and guidance, as well as Office of Management and Budget (OMB) memoranda. NIST Special Publication (SP) 800-53 is fully incorporated into Department policies and it provides the core set of controls implemented at the system level. Specifically, in 2006, the Department completed a year-long system accreditation project and the number of systems that are fully accredited rose from 24% to 95%. As a result of this effort, systems now have documented plans in place for implementing the NIST recommended IT security controls, and the effectiveness of these controls has been verified for each system.

12. When the Department purchases software, do procurement documents require that the purchased software operates effectively on the secure configurations? If not, what does the Department do when a purchased package requires security configurations to be weakened in order to run the purchased application?

The Homeland Security Acquisition Regulations require vendors to comply with all Department IT security policies (specifically 4300A), including the Department's operating systems configuration guidance. (Note: The Department has published hardening guidance for all operating systems that are currently in use or that are planned for in future implementations.) Waivers to this policy expressly require risk acceptance and mitigation measures and a plan for bringing the system into compliance.

13. What are your top three initiatives for securing the Department for 2008? How do you measure those goals?

The Department is currently pursing a number of initiatives to improve our overall Information Security posture. Among these, the top three are:

- 100% FISMA compliance
- Consolidated networks and datacenters
- HSPD-12 implementation

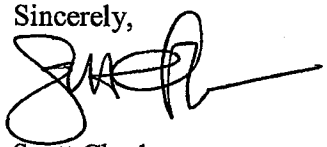
Full compliance with FISMA will allow the Department to fulfill the goals of the act, including implementing cost-effective, risk-based information security programs; providing improved, cost-effective application of IT security controls; allowing for more consistent, repeatable security control assessments; and providing more complete, reliable, and real-time information to the DHS leadership. This initiative is currently underway and being tracked through monthly FISMA Scorecards for each Component. The overall success will be realized by an increased Department-wide OMB FISMA score.

Consolidation of DHS networks and datacenters is also a top priority. The Department currently operates a number of scattered networks and datacenters of varying capabilities, making it difficult to maintain consistent standards, increasing costs and forcing duplication of effort. Consolidation will allow for improved standardization, giving the Department a greater ability to apply more effective and consistent security policies, reducing operations and maintenance costs, and allowing DHS to better focus efforts and resources. Overall success will be realized through improved security, consistent capabilities, and decreased costs.

HSPD-12 implementation is another priority. This initiative will give the Department an increased identity verification capability for its employees and contractors, allowing for tighter physical and logical access controls. Furthermore, HSPD-12 will give DHS the ability to implement full two-factor authentication for all Government and Contractor personnel, as well as providing a secure, reliable interoperability capability with all other Federal agencies.

I hope that I have answered your questions to your satisfaction. Should you require any additional information or have any additional questions, please contact my chief of staff, Michael Butcher, at (202) 447-3734.

Sincerely,



Scott Charbo
Chief Information Officer

cc:
Michael Jackson, Deputy Secretary
Paul Schneider, Under Secretary for Management
Robert West, Chief Information Security Officer

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 31, 2007

The Honorable Scott Charbo
Chief Information Officer
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Charbo:

Thank you for your timely response to the April 30, 2007 letter from this Committee. I have several follow-up questions based on the materials you provided:

1. The network topology diagram provided to the Committee is incomplete. Please provide the full network topology diagram.

2. Has the Department identified any security concerns as it moves forward with the "OneNET" proposal, and, if so, what plans are in place to remedy any vulnerabilities prior to the convergence of the networks?

3. Please provide a list of all mitigation actions tracked within the Department's Trusted Agent FISMA (TAF) tool, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

4. Please provide a list of all vulnerabilities that are recorded and tracked within the TAF Plan of Action and Milestone (POA&M) folder, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

5. During a meeting with Committee staff, you stated that you are authorized to reduce funding to agency components that do not mitigate their POA&M vulnerabilities in a timely fashion. Please provide a list of funding reductions or recommendations for funding reductions that you made to Secretary Chertoff. Please also provide a narrative of Secretary Chertoff's response to your recommendations.

6. If you have not provided funding cut recommendations to the Secretary, please provide a list of any agency components that have not mitigated their POA&M vulnerabilities and a narrative explaining your decision not to recommend a funding reduction.

7. According to the Department's policy on Contractors and Outsourced Operations, "components shall conduct reviews to ensure that the IT security requirements in the contract are implemented and enforced."[1] When was the last Department-wide review of these contracts? Were these reviews conducted by component CIOs or by personnel within your line of authority? What vulnerabilities were identified in the review and when were they remedied? Please provide the Committee with each component review of their outsourced operations, as well as the Departmental review of the components' work.

8. According to the Department's policy on Risk Management, "components shall conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment have been made, or every three years, whichever comes first."[2] Please provide these risk assessments, including the dates the assessments were conducted.

9. According to the Department's policy on IT Security Review and Assistance, "the DHS CISO shall conduct IT security review and assistance visits throughout the Department to determine the extent to which the Component security programs comply with IT security policy, standards, and procedures."[3] When were these security reviews completed? How many components passed or failed this review?

10. The Department's policy on "Wireless Systems" requires "annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions."[4] Please provide the Committee with those assessments.

11. When did the Department last audit the MCI MPLS Cloud or the Sprint MPLS Cloud? What were the results of the audit? Did the Department require MCI or Sprint to mitigate vulnerabilities?

12. The Committee requested and received a list of the FY 2005 and FY 2006 incidents reported to the Department's Security Operations Center (DHS SOC).

    a. Please define a "classified data spill." How is this incident different from an incident where a Department employee sends a classified email through a non-classified system?

    b. Please explain what disciplinary actions were taken against the contractors in DHS Incident # 2006-08-031.

    c. Please provide a list of the FY 2007 incidents reported to the DHS SOC.

---

[1] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 19.
[2] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 22.
[3] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 22.
[4] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 37.

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, I request a response in writing by not later than June 15, 2007. If you have any questions, please contact, Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security at (202) 226-2616.

Sincerely,

Bennie G. Thompson
Chairman

BGT/jso

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

Homeland Security

June 15, 2007

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

06-18-07P04:23 RCVD

Dear Mr. Chairman:

It is my pleasure to provide the following responses to your committee's May 31, 2007 follow-on request for information concerning the Department of Homeland Security's (DHS) information technology security policies and procedures (Attachment 1).

1. **The network topology diagram provided to the Committee is Incomplete. Please provide the full network topology diagram.**

Please find the attached Department of Homeland Security (DHS) OneNet topology diagram. The diagram represents the Department's current infrastructure and details OneNet, DCN, and the Component Connectivity (Attachment 2). A second diagram shows the Department's A LAN (Attachment 3). Additional topology diagrams will be provided to your office by Tuesday, June 19, 2007.

2. **Has the Department identified any security Concerns as it moves forward with the "OneNET" proposal, and, if so, what plans are in place to remedy any vulnerabilities prior to convergence of any networks.**

The OneNet project is currently managed by the DHS Infrastructure Transformation Program (ITP) within the Office of the Chief Information Officer (DHS CIO). Infrastructure Operations, also an office within the DHS CIO organization, is responsible for the ITP, and provides ongoing assurance that security controls are duly executed in conformance with Chief Information Security Officer (CISO) policies and acts as the OneNet Designated Accrediting Authority (DAA).

The OneNet Certification and Accreditation (C&A) was completed during the implementation stage and achieved an acceptable risk posture in January 2007. An Authority to Operate (ATO) was subsequently issued and residual vulnerabilities, discovered during the accreditation security testing and evaluation (ST&E) process, were entered into the system's Plan of Actions and Milestones (POAM), provided as Attachment 4. POAM items are being addressed in accordance with DHS 4300A Attachment H, *Plans of Actions and Milestones Process Guide*, provided as Attachment 5.

The following program issue is being addressed by the DHS CIO in partnership with the DHS service provider, U.S. Customs and Border Protection (CBP).

During the accreditation security testing and evaluation process, we assessed that the security control family for audit collection, retention, review, and management was not in place. Customs and Border Protection, responsible through the ITP Charter for One Service Delivery, is fully aware of the audit deficiencies and has a high level security project plan (POAM) to correct them. The lack of full audit management does not pose a risk to the Component Agencies, neither currently nor when they have complete network convergence. Nonetheless, successfully addressing this issue will provide the Department with further empirical indicators as a security quality assurance measure that the network has the appropriate security and operational administrative control procedures in place.

3. **Please provide a list of all mitigation actions tracked within the Department's Trusted Agent FISMA (TAF) tool, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.**

A Department-wide POAM is provided in Attachment 4.

4. **Please provide a list of all vulnerabilities that are recorded and tracked within the TAF Plan of Action and Milestone (POA&M) folder, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.**

A Department-wide POAM is provided in Attachment 4.

5. **During a meeting with the Committee staff, you stated that you are authorized to reduce funding to agency components that do not mitigate their POA&M vulnerabilities in a timely fashion. Please provide a list of funding reductions or recommendations for funding reductions that you made to Secretary Chertoff. Please also provide a narrative of Secretary Chertoff's response to your recommendations.**

During the meeting with the Committee staff, the response to the question of the Chief Information Officer's authority and how he can influence a component's progress was answered in three parts by the Chief Information Officer. To clarify, the Chief Information Officer can make recommendations to the Secretary for budget reductions, but he cannot reduce budgets himself. This three part answer was based on the Secretary's changes to Management Directive 0007.1, *Information Technology Integration and Management*. Additional information follows:

Secretary Chertoff recently instituted changes in the oversight function of the Chief Information Officer for the Department of Homeland Security (DHS). DHS published a revised Management Directive 0007.1 in March 2007, improving the ability of the Chief Information Officer to

manage and influence the Department's information technology programs. Included in these changes were:

1. Components must provide their information technology (IT) budgets annually to the DHS Chief Information Officer for review; I will then make recommendations to the Secretary for final budget submissions to the Office of Management and Budget.

2. Any proposed IT acquisition greater than $2.5 million must be reviewed and approved by the DHS Chief Information Officer. IT acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.

3. Before IT investment proposals greater than $2.5 million are submitted to the DHS Chief Information Officer for approval, the Department's Enterprise Architecture Board must approve the investment and certify its alignment with the Department's enterprise architecture.

4. The DHS Chief Information Officer will approve the hiring of Component Chief Information Officers, as well as set and approve their performance plans, ratings, and annual award compensation.

As part of the process of reviewing and making recommendations for component IT budgets, I also take into account components' performance in mitigating their POAM vulnerabilities.

Included in this improved Management Directive is the inherent ability to influence the budget in areas where a component's information security posture is weak. While I have never recommended that a component's budget be reduced due to a lack of success in a POAM, I have been able to provide guidance and direction to the components that are not satisfactorily progressing in their POAMs. Since March 2007, when the Management Directive gave these additional powers to the Chief Information Officer, I have written letters to the directors of three components pointing out ways they could improve their FISMA scores (See these letters in Attachment 6).

Indeed, it is not always the best policy to reduce an IT budget if a POAM is not being satisfactorily met. My experience has shown that the components are in fact making efforts to resolve their problems and that the lack of financial means to mitigate vulnerabilities is their primary obstacle to success. We would want to provide encouragement and support to components so that they can obtain additional resources to ensure success.

6. **If you have not provided funding cut recommendations to the Secretary, please provide a list of any agency components that have not mitigated their POA&M vulnerabilities and a narrative explaining your decision not to recommend a funding reduction.**

A Department-wide POAM is provided in Attachment 4.

Please see the answer to question 5.

7. **According to the Department's policy on Contractors and Outsourced Operations, "components shall conduct reviews to ensure that the IT security requirements in the contract are implemented and enforced." When was the last Department-wide review of these contracts? Were these reviews conducted by component CIOs or by personnel within your line of authority? What vulnerabilities were identified in the review and when were they remediated? Please provide the Committee with each component review of their outsourced operations, as well as the Departmental review of the components' work.**

The Department has a total of 717 systems in its inventory. This includes 501 government systems and 216 contractor systems. The Department mandates the testing of information systems security controls for all systems, government and contractor alike, using the National Institute of Standards and Technology (NIST) Special Publication 800-53 (SP 800-53) methodology. Please refer to Attachment 7, summary of NIST SP-800-53 assessment results for a summary of these assessments. Contracting officers and their technical representatives (COTRs) also review contractor performance, including compliance with information security requirements.

Additionally, the Department ensures that IT security requirements are included and enforced in all contracts. To that end, the DHS CIO implemented the IT Acquisition Review (ITAR) process that provides for the DHS CIO's review of all IT acquisitions of $2.5M or more. Public Law 109-295 requires that "no funds be made available for obligation for any information technology procurement of $2.5M or more without approval of the DHS CIO."

In support of this effort, the CISO developed review criteria and evaluates every Purchase Request (PR) to ensure that the appropriate personnel and information security requirements are included prior to CIO approval and release. The CISO staff has conducted and adjudicated more than 130 PR reviews since October 1, 2006. Please refer to Attachment 8, Summary of Information Technology Acquisition Reviews for a summary of these reviews.

DHS Management Directive 0007.1 requires the DHS CIO to "review and approve all Component IT budgets." The CISO staff completed security reviews for more than 375 investments (levels 1 through 4) in April 2007 and provided the security scores to the Capital Planning and Investment Control (CPIC) in support of this requirement. A summary of the results is presented in Attachment 9, Contractor Monitoring Summary.

8. **According to the Department's policy on Risk Management, "components shall conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment have been made, or every three years, whichever comes first." Please provide these risk assessments, including the dates the assessments were conducted.**

A complete set of risk assessments is provided in Attachment 10. Please be aware that this information is considered highly sensitive and should not be released.

9. **According to the Department's policy on IT Security Review and Assistance, "the DHS CISO shall conduct IT security review and assistance visits throughout the Department to determine the extent to which the Component security programs comply with IT security policy, standards, and procedures." When were these security reviews completed? How many components passed or failed this review?**

The Department conducts security review and assist visits on an ongoing basis. The Office of Information Security (OIS) IT Security Compliance Team reviews and assesses Certification and Accreditation (C&A), including compliance with the Federal Information Systems Management Act (FISMA).

Documents are reviewed on a pass/fail basis against criteria described in the FY07 Information Security Performance Plan, provided as Attachment 11, and the Compliance Team provides Components with feedback on how to raise the quality of systems security, if required.

Plans of Action and Milestones (POAMs) are reviewed monthly and assessed for compliance with OMB guidance and against criteria described in the FY07 Performance Plan. All systems are graded on a pass/fail basis and the Compliance Team tracks Government Accounting Office (GAO), Office of the Inspector General (OIG) and financial audit findings to ensure that appropriate POAMs have been developed for each recommendation. It also monitors POAMs through completion.

The overall FISMA compliance status for each Component and results of compliance reviews are compiled in a monthly scorecard and distributed to Department ISSMs and CIOs.

Training and assistance provide tailored support designed to help individual Components address compliance issues. In most cases, this involves working directly with Component Information System Security Managers and Officers (ISSMs and ISSOs) in order to address weaknesses. Security training and assistance visits for FY07 have included:

- Training Activities
  - C&A
  - Risk Management System (RMS) and TrustedAgent FISMA (TAF)
  - POAM
  - Security Awareness
  - Role Based Training – Financial System Workshop

- Face-to-face and hands-on assistance to help Components understand requirements and conduct activities to ensure improved compliance in the following areas
  - C&A
  - TAF
  - POAM
  - Financial Audit Remediation Activities

Details for all the activities are provided in Attachment 12.

10. The Department's policy on "Wireless Systems" requires "annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions." Please provide the Committee with those assessments.

Assessments of the wireless or wired infrastructure are to be completed every three years per Section 3.8.b of DHS Sensitive Systems Policy 4300A version 5.1. The exception to this rule occurs when there is a major configuration change to a system, which requires an immediate re-assessment. Security assessment responsibility is a Component-level activity performed by the Component CIO organizations as part of the DHS security management program.

The Department's Security Certification and Accreditation process, in accordance with DHS and NIST security policies and standards, includes the wireless environment when necessitated by mission need in the System Security Life Cycle for each given General Support System. Security assessments for operational wireless systems have been included, as applicable, in the full Security Risk Assessments provided to the Committee in response to Question 8 of your Memorandum.

The DHS Enterprise Architecture recognizes the pervasive need and use of Wireless Systems and has established a Wireless Security Board in collaboration with the DHS Chief Information Security Officer for promulgating wireless policy, standards and assessments for the wireless environment.

11. When did the Department last audit the MCI MPLS Cloud or the Sprint MPLS Cloud? What were the results of the audit? Did the Department require MCI or Sprint to mitigate vulnerabilities?

The Department has reviewed the security and network operational environments for the two OneNet provided carriers. In 2006, the Department reviewed the carrier services at Sprint during a visit with the network steward. The review focused on management and operational issues. However, the review did not cover a technical assessment (security test and evaluation) because the General Services Administration (GSA) is responsible for technical assessments and security validation under both FTS-2001 and Networx. The security inherent in the Dynamic Multiple Virtual Private Network suite of protocols fully protects the confidentiality and integrity of all information transiting the OneNet. The Department has Service Level Agreements with each carrier, attesting that they have established and will maintain conformance with the applicable DHS security controls and availability metrics, which reduces any potential attack on network availability. GSA serves as the government-wide Contracting Officer for the FTS-2001 contract and the upcoming Networx contract and is for technical assessments and security validation of the environment. GSA has agreed, during the Networx requirements gathering process, to assume the responsibility for ensuring that the carriers meet or exceed the applicable security requirements of the National Institute of Standards and Technology once the final contract is awarded.

12. The Committee requested and received a list of FY 2005 and FY 2006 incidents reported to the Department's Security Operations Center (DHS SOC).

a. Please define a "classified data spill." How is this incident different from an incident where a Department employee sends a classified email through a non-classified system?

A classified data spill, also referred to as a "classified information spill," or a "collateral information spill," occurs whenever classified information is brought onto a network not approved for the level of classification commensurate with the sensitivity of the information. This can happen through a variety of vectors, including email, Compact Discs, removable media or manual data entry. The Department goes to great lengths to prevent direct electronic transfer between networks, however, when a classified spill occurs, it is usually the result of personnel not following proper classified data handling procedures. A Department employee sending classified information via email through a non-classified system is a type of classified data spill.

Under current policy, when a Component or Component Security Operations Center (SOC) becomes aware of a suspected or confirmed spillage, it is reported to the DHS SOC either in person or via telephone without delay. Other methods of reporting (Fax, email, DHS SOC Online) are not allowed for this type of incident because they provide additional electronic trails that must also be sanitized, thereby increasing the risk that the information will become accessible to unauthorized persons. Once notified, the DHS SOC coordinates the appropriate required actions.

b. Please explain what disciplinary actions were taken against the contractors in DHS Incident #2006-08-031.

Incident 2006-08-031 was entered as a minor incident whereby unauthorized users had attached personal computers to the government network. No access was obtained, and the incident was closed with the following additional action: "Laptops were removed, personnel were escorted off of the premises and training was issued to those who allowed them access to the area.

The full incident report is provided in Attachment 13.

c. Please provide a list of the FY 2007 incidents reported to the DHS SOC.

A list of incidents from October 1, 2006 to June 4, 2007 is provided in Attachment 14.

Thank you for the opportunity to provide the information to you and your committee. While information security is not perfect at the Department, we have come a long way from our initial attempts to ensure the security of our data and information. I look forward to working with this committee and Congress in the future to ensure that information security reaches the highest levels of competence at the Department.

Enclosures have been provided on a CD-ROM, with a password to the documents provided under separate cover.

Should you require any additional information or have any additional questions, please contact the Chief of Staff for the DHS CIO, Michael Butcher at (202) 447-3734.

Sincerely,

Scott Charbo
Chief Information Officer

Enclosures

cc:
Michael Jackson, Deputy Secretary
Paul A. Schneider, Under Secretary for Management

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 27, 2007

Scott Charbo
Chief Information Officer
Department of Homeland Security
Washington, D.C. 20528

Robert West
Chief Information Security Officer
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Charbo and Mr. West:

The House Committee on Homeland Security is currently conducting a review of federal information system security. On July 18, 2007, the Department of Homeland Security's Inspector General released a troubling report about information technology management at the Department. The "Information Technology Management Letter for the DHS FY 2006 Financial Statement Audit" contains observations and recommendations related to information technology internal controls on the Department's financial management systems. Unfortunately, the audit indicates that significant vulnerabilities remain prevalent on Department systems.

While some Department components demonstrated improvement over the previous year, auditors found that most did not measurably enhance their security posture. During the 2006 IT testing, auditors identified over 200 vulnerable conditions on financial management networks that were in need of mitigation. Though the Department closed 44 percent of those risks, more than 150 new findings were discovered this year. The vulnerabilities identified by the audit include: 1) excessive access to key Department financial applications; 2) misconfigured logical security controls to key Department financial applications and support systems; and 3) application change control processes that are inappropriate, and in other locations not fully defined, followed, or effective. Unfortunately, failing to mitigate these conditions jeopardizes the integrity of the Department's financial systems.

This recent report on financial systems follows several studies issued by the Inspector General in 2006 that examined information security at Department components. For instance, in June 2006, the Department of Homeland Security Inspector General released a report assessing the strengths and weaknesses of the

Science and Technology Directorate's (S&T) laptop computer security controls. The report found that "significant work remains for S&T to further strengthen the configuration, patch, and inventory management controls necessary to secure its data stored on government-issued laptop computers." Weaknesses at components like S&T can have significant consequences to data integrity throughout the Department.

The Committee is deeply concerned that the vulnerable conditions highlighted in recent reports by the Inspector General may facilitate espionage on the Department's computers. We ask that you please provide answers to the following questions:

1. Has there ever been an incident characterized as an "Unauthorized Access" (US-CERT Incident Category 1) or "Malicious Code" (US-CERT Incident Category 3) that took place on a network, a computer, or a computer user account associated with or attributed to the Office of Procurement Operations or the S&T Directorate? Please provide all Incident Assessment Forms and associated reports for each of these incidents.

2. Has a hacking tool or password dump utility ever been loaded on a network, a computer, or a computer user account in the Office of Procurement Operations or the S&T Directorate? If so, what level or position was the user associated with the machine? If not, have any computers in the Office of Procurement Operations or S&T Directorate been connected to a computer containing known malicious logic or hacker tools?

3. Has an infected machine associated with the Office of Procurement Operations or the Science and Technology Directorate ever exfiltrated (transmitted out) information? If so, did the Department perform independent verification and validation assessments to identify a nation state hacker presence? What was the result of these assessments?

4. In previous communications with the Committee, your office provided a list of cybersecurity incidents reported to the Department's Security Operations Center (SOC) from FY 2005-2007. During the June 20, 2007 Emerging Threats, Cybersecurity, and Science and Technology Subcommittee hearing, members discussed several of these incidents that occurred during 2006. Please provide the Committee with all documents, communications, or correspondence regarding the following incidents, including electronic correspondence between and among contractor groups associated with these incidents:

    - DHS Incident #2006-09-030
    - DHS Incident #2006-09-013
    - DHS Incident #2006-09-041
    - DHS Incident #2006-08-031

- DHS Incident #2006-08-011
- DHS Incident #2006-06-047
- DHS Incident #2006-06-031

Pursuant to Rule X (3)(g) and Rule XI of the Rules of the House of Representatives, we request a response in writing by not later than August 27, 2007. If you have any questions, please contact Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security, at (202) 226-2616.

Sincerely,

Bennie G. Thompson
Chairman

James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology

BGT/jso

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

Homeland Security

Aug 27, 2007

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

09-04-07P05:22

Dear Mr. Chairman:

Thank you for your letter dated July 27, 2007, in which you requested information concerning the July 18, 2007 Department of Homeland Security (DHS) Office of Inspector General report entitled, *Information Technology Management Letter for the DHS FY 2006 Financial Statement Audit* (Enclosure A). This letter provides a response to the four questions you posed regarding possible computer incidents at DHS:

1. **Has there ever been an incident characterized as an "Unauthorized Access" (US-CERT Incident Category 1) or "Malicious Code" (US-CERT Incident Category 3) that took place on a network, a computer, or a computer user account associated with or attributed to the Office of Procurement Operations or the S&T Directorate? Please provide all Incident Assessment Forms and associated reports for each of these incidents.**

The DHS Security Operations Center (SOC) has three reports of "Unauthorized Access" and one report of a "Malicious Code" incident pertaining to the Science and Technology (S&T) Directorate. There are none specifically pertaining to the Office of Procurement Operations. The S&T "Unauthorized Access" reports are provided in Enclosure B, C, and D, and the "Malicious Code" report in Enclosure E. Please note that one of the "Unauthorized Access" reports (2005-07-001) stemmed from miscommunication between personnel, and not from an outside attempt. The user was correct in reporting it.

2. **Has a hacking tool or password dump utility ever been loaded on a network, a computer, or a computer user account in the Office of Procurement Operations or the S&T Directorate? If so, what level or position was the user associated with the machine? If not, have any computers in the Office of Procurement Operations or S&T Directorate been connected to a computer containing known malicious logic or hacker tools?**

A password dump utility was discovered on 15 machines in September of 2006. Affected machines belonged to persons with no special user privileges. The machines were quickly identified,

removed, and replaced with newly-imaged machines, and additional steps were taken to prevent further occurrences.

While this incident remains under investigation, preliminary analysis indicates that no information was transferred to unauthorized persons. The incident report is provided in Enclosure C.

3. **Has an infected machine associated with the Office of Procurement Operations or the Science and Technology Directorate ever exfiltrated (transmitted out) information? If so, did the Department perform independent verification and validation assessments to identify a nation state hacker presence? What was the result of these assessments?**

Several infected machines were discovered in September of 2006. It was subsequently determined that one machine had established a connection to an IP address of interest as identified by US-CERT, an Internet Service Provider located in Dallas, TX. This is the same incident referred to in response to question 2 (see Enclosure C). This incident remains under investigation.

4. **In previous communications with the Committee, your office provided a list of cybersecurity incidents reported to the Department's Security Operations Center (SOC) from FY 2005-2007. During the June 20, 2007 Emerging Threats, Cybersecurity, and Science and Technology Subcommittee hearing, members discussed several of these incidents that occurred during 2006. Please provide the Committee with all documents, communications, or correspondence regarding the following incidents, including electronic correspondence between and among contractor groups associated with these incidents:**

- **DHS Incident #2006-09-030** (Enclosure F)
- **DHS Incident #2006-09-013** (Enclosure G)
- **DHS Incident #2006-09-041** (Enclosure C)
- **DHS Incident #2006-08-031** (Enclosure H)
- **DHS Incident #2006-08-011** (Enclosure I)
- **DHS Incident #2006-06-047** (Enclosure J)
- **DHS Incident #2006-06-031** (Enclosure K)

The requested incident information is provided in Enclosures C and F-K. Some general comments regarding each incident are as follows:

Incident Number	Reported Anomaly	Conclusion following Investigation	Remedial Actions
2006-09-030-Malicious_Logic (F)	Suspicious Beaconing Activity	Some malware found.	Affected equipment was taken offline and re-imaged; disabled appropriate RSA tokens and blocked relevant IP addresses at the firewall.
2006-09-013-FEMA_Website (G)	Suspected compromise of Federal Emergency	No evidence of compromise was found.	The legacy web server was replaced with

Incident Number	Reported Anomaly	Conclusion following Investigation	Remedial Actions
	Management Agency website		updated hardware and software for good measure.
2006-09-041-Password Dump (C)	A password dumping utility was found on several DHS machines	This investigation is presently ongoing.	Machines replaced and passwords changed.
2006-08-031-Unauthorized_Access (H)	Attempted unauthorized access	Personnel had plugged unauthorized equipment into a DHS network port. Equipment did not access the DHS network.	Personnel were escorted off the premises and training was provided to those who had allowed them access to the area.
2006-08-011-Sprint_DNS (I)	Misconfiguration of DNS firewall rules	Sprint had enabled a firewall rule that would allow traffic over Transmission Control Protocol and User Datagram Protocol port 53 out to the Internet.	Sprint enabled blocking of Domain Name System and DHS management was informed of the situation.
2006-06-047-Sprint_Firewall (J)	Misconfiguration of ICMP firewall rules	Sprint had enabled a firewall rule that would allow ping and TRACERT traffic in from and out to the Internet.	Sprint enabled blocking of Internet Control Message Protocol and DHS management was informed of the situation.
2006-06-031-Backdoor.Nanif.E (K)	Malicious code found on several US Coast Guard machines	Anti-Virus (AV) systems did not detect the infection initially.	Affected machines were reimaged and temporary blocking of certain types of attachments (zip files) was initiated. AV signatures were updated.

An identical letter has been sent to the Chairman of the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security. Should you require additional information or have any additional questions, please contact me at (202) 282-9251.

Sincerely,

Robert West

Robert West
Chief Information Security Officer

Enclosures