EDO Principal Correspondence Control

FROM: DUE: 04/16/08

EDO CONTROL: G20080230
DOC DT: 03/27/08
FINAL REPLY:

Senator Thomas R. Carper
Senator Norm Coleman
(OCA)

TO:

OPA

FOR SIGNATURE OF : ** GRN ** CRC NO:

DESC:

Post Hearing Qs from the March 12, 2008 Hearing on Protecting IT and Secure Sensitive Information (Due to OCA: 4/22/08) (EDATS: OEDO-2008-0271)

ROUTING:

Reyes
Virgilio
Mallett
Ash
Ordaz
Cyr/Burns
Boyce, OIS
Schmidt, OCA
Landau, OEDO

DATE: 04/02/08

ASSIGNED TO: CSO

CONTACT: Howard

SPECIAL INSTRUCTIONS OR REMARKS:

Use the attached format. Coordinate with OIS. Provide input via e-mail to Mindy Landau, OEDO by April 16, 2008.

Due to OEDO: 4/16/08
Due to OCA: 4/22/08
Due to Congress: 4/30/08

Template: EDO-001

E-RIDS: EDO-01

EDATS

Electronic Document and Action Tracking System

EDATS Number: OEDO-2008-0271 **Source:** OEDO

General Information

Assigned To: CSO **OEDO Due Date:** 4/16/2008 5:00 PM

Other Assignees: **SECY Due Date:** NONE

Subject: Post Hearing Q's from the March 12, 2008 Hearing on Protecting IT and Secure Sensitive Information (Due to OCA: 4/22/08)

Description:

CC Routing: OIS; OCA

ADAMS Accession Numbers - Incoming: NONE **Response/Package:** NONE

Other Information

Cross Reference Number: G20080230 **Staff Initiated:** NO

Related Task: **Recurring Item:** NO

File Routing: EDATS **Agency Lesson Learned:** NO

Roadmap Item: NO

Process Information

Action Type: Post **Priority:** Medium

Sensitivity: None

Signature Level: No Signature Required **Urgency:** NO

OEDO Concurrence: NO

OCM Concurrence: NO

OCA Concurrence: NO

Special Instructions: Use the attached format. Coordinate with OIS. Provide input via e-mail to Mindy Landau, OEDO by April 16, 2008.

Document Information

Originator Name: Sen. Thomas R. Carper/Sen. Norm Coleman **Date of Incoming:** 3/27/2008

Originating Organization: Congress **Document Received by OEDO Date:** 4/2/2008

Addressee: OPA **Date Response Requested by Originator:** 4/30/2008

Incoming Task Received: Other

Post-Hearing Questions for the Record

"Agencies in Peril: Are We Doing Enough to Protect IT and Secure Sensitive Information?"
March 12, 2008

<u>Questions for the Record from Senator Thomas R. Carper</u>

1.) Mr Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a short explanation of why you chose what you did.

2.) In the past year, the Administration has implemented a lot of initiatives to help secure our sensitive information and reduce costs. One of these initiatives is called the Information Systems Security Line of Business. I understand that this initiative will standardize information security education and reporting government-wide.

   a. How is your agency taking advantage of these Lines of Business?
   b. And do you think there are more opportunities for your agency, or others, to take advantage or improve these initiatives?
   c. In addition, do you think there may be more ways we can standardize information security practices to reduce costs and increase security?

3.) Also, I understand that there are some new cyber security initiatives that have deadlines soon or were recently supposed to be completed such as the Federal Desktop Core Configuration, Trusted Internet Connection, transition to IPv6, etcetera.

   a. How are your specific agencies coping with these transitions?
   b. And do you have comprehensive plans in place to be fully compliant with these initiatives when OMB has asked?
   c. Is your agency struggling with complying with any of these initiatives?
   d. If so, what needs to happen before you are compliant with these transitions?

4.) Ensuring appropriate executive level buy-in is critical to any mission critical area, especially information security. In your own agencies, have the roles of Chief Information Officers and Chief Information Security Officers been elevated to an effective level in the organization to put in place effective information security policies and procedures and enforce security?

   a. In your opinion, what is an effective level of authority to place our CIOs and CISO's within a federal agency of your size and mission?

Post-Hearing Questions for the Record
Submitted to Daren Ash
From Senator Norm Coleman

"Agencies in Peril: Are we Doing Enough to Protect Federal IT and Secure Sensitive Information?
March 12, 2008

1. At the end of February, Senator Collins and I sent a letter to 24 federal agencies highlighting the findings of the GAO on Protecting Sensitive Agency Information. We also requested a timeline in writing for when each agency expected to be in compliance with all the OMB Memoranda focused on protecting Personally Identifiable Information.

   - **In your testimony you discussed how your agencies were complying with pieces of OMB Memoranda on protecting PII (see list below). Are your agencies fully compliant with all the OMB recommendations on protecting PII issued before the start of this year?**

Date:	*Report*	*Title*
02/11/2005	*M-05-08*	*Designation of Senior Agency Officials for Privacy*
05/22/2006	*M-06-15*	*Safeguarding Personally Identifiable Information*
06/23/2006	*M-06-16*	*Protection of Sensitive Agency Information*
07/12/2006	*M-06-19*	*Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
07/17/2006	*M-06-20*	*FY2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
05/22/2007	*M-07-16*	*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

   - **If not, do you have a timeline for when you will be fully compliant? Do you know when your agencies will be sending us the status and timeline in writing for reaching compliance with all the OMB recommendations?**

   - **Would you say that it is a high priority for all your agencies to be in compliance with the OMB memoranda on Personally Identifiable Information?**

   - **Is there anything Congress can do to help your agencies comply with the OMB guidance? Is it a matter of funding or is additional legislation needed?**

2. A growing band of civilian units inside China is writing malicious code and training to launch cyber strikes into enemy systems. As for many of these units, the first enemy is the Department of Defense, the Department of Homeland Security and our nations' law enforcement agencies. Pentagon officials say there are more than three million daily scans of the Global Information Grid, the Defense Department's main network artery, and that the U.S. and China are the top two originating countries. I was disturbed by the March 7, 2008, CNN article entitled, *Chinese hackers: No site is safe,* which provided disconcerting insights into the People's Liberation Army's efforts to penetrate the Pentagon's IT network and other sensitive U.S. Government computer networks vowing that and I quote, "No Web site is one hundred percent safe".

- **Right now China and more than 20 other nations possess dedicated cyber warfare computer attack programs – and that number doesn't include terrorist organizations. Can you please elaborate for me on exactly what your agency is pro-actively doing to prepare for the cyber warfare threat? Are you doing anything beyond the OMB memorandums to pro-actively address this challenge?**

3. Some of the more notable breaches to personal identifying information maintained by the government have occurred away from the agency, usually while an employee is on travel or at home. Additionally, laptop computers are frequently used to conduct government business while travelling. Many of these computers contain sensitive agency or personal information. Thefts of laptops are very common, not to get the information but to get the device.

   - **What efforts have been taken through regulatory or policy guidance to limit the number of employees who have outside access to sensitive information or to limit how much sensitive information they can have access to at a time?**

   - **What efforts have been taken to make these computer system more secure, such as through the use of a boot-up password or token, or encryption of the data? Are there any requirements regarding the strength of the passwords or encryption used?**

FORMAT FOR CONGRESSIONAL Q&As

QUESTION 6. Congressional questions are assigned to various offices for preparation of the answers.

(A) What is the typing format for responding to Congressional questions?

ANSWER.

Q&As are to be typed on word processing equipment (WordPerfect) and provided to the EDO both by hard copy and a 3.5 inch diskette (as directed on Green Control Ticket under Special Instructions or Remarks). Type each Q&A as a separate job (including multiple parts, [A, B, C, etc.]) to aid in later revisions and transmission of Q&As to Congressional Affairs. Use 11 pitch, Arial type style, initial caps only, and double spacing. Use four spaces between each paragraph. Side margins are 1-inch for both left and right; and 1-inch for the top and bottom margins. Do not use a required return after each typed line.

At the bottom right margin on each page in the footer text, indicate Committee, originating Office (not Division or Branch). Current date should appear directly below the Committee/Office. Subsequent revisions should reflect the revised date.

If succeeding pages are required in answering the question, the question number and page number should be typed in the header margin text area, so that it appears at the top of each succeeding page (as shown above).

If enclosures are to be included with a response, indicate on Q&A (as shown below) and type question number and part (A, B, C, etc., as appropriate) on each enclosure. Provide an electronic copy of the enclosure, if possible.

Enclosure:
Sample Q&A Format