



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

NOV 8 2012

OFFICE OF
INSPECTOR GENERAL

The Honorable Rafael Moure-Eraso, Ph.D.
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
2175 K. Street, NW, Suite 400
Washington, DC 20037-1809

Dear Dr. Moure-Eraso:

Enclosed is the completed Fiscal Year 2012 Federal Information Security Management Act Reporting Template, as prescribed by the U.S. Department of Homeland Security (DHS). The template synthesizes the results of information technology security work performed by KPMG, LLP, under the direction of the U.S. Environmental Protection Agency, Office of Inspector General (OIG).

In accordance with DHS reporting instructions, the OIG is forwarding this information to you for submission to the Director of DHS.

If you or your staff have any questions regarding the enclosed report, please contact me at (202) 566-0899 or heist.melissa@epa.gov; or Rudolph Brevard, Director, at (202) 566-0893 or brevard.rudy@epa.gov.

Sincerely,

A handwritten signature in black ink that reads "Melissa M. Heist". The signature is written in a cursive style.

Melissa M. Heist
Assistant Inspector General for Audit

Enclosure

OMB Micro Agencies Questions

1. System Inventory

1.1 For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low) in this question, provide the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below. (Organizations with below 5000 users may report as one unit.)

	1.1A Organization Operated Systems			1.1b Contractor Operated Systems			1.1c Systems (from 1.1a and 1.1b) with Security ATO		
	H	M	L	H	M	L	H	M	L
FIPS 199 Category									
CSB	0	1	0	0	0	0	0	1	0

1.2 For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Organization operational, information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below.

	1.2a Systems utilizing cloud computing resources		1.2b Systems utilizing cloud computing resources (1.2a) with a Security Assessment and Authorization		1.2c Systems in 1.2a utilizing a FedRAMP authorized Cloud Service Provider	
	M	L	M	L	M	L
FIPS 199 Category						
CSB	0	0	0	0	0	0

2. Asset Management

2.0 Provide the total number of organization hardware assets connected to the organization's unclassified network	279
2.1 Provide the number of assets in 2.0, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	198
2.2 Software Assets: Can the organization track the installed operating system Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0.	Yes (6)

<p>2.2a Can the organization track (for each installed operating system Vendor, Product, Version, and patch- level combination in 2.4) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning?.</p>	<p style="text-align: center;">No</p> <p>As of FY 2013, CSB made network updates that allows it to track (for each installed operating system Vendor, Version, and patch level combination in 2.2) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning.</p>
--	---

3. Configuration Management

<p>3.1 For each operating system Vendor, Product, Version, and patch-level combination referenced in 2.2, report the following:</p>	
<p>3.1a Whether an adequately secure configuration baseline has been defined</p>	<p style="text-align: center;">Yes (4/6)</p>
<p>3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).</p>	<p style="text-align: center;">109</p>
<p>3.1c For what percentage of the applicable hardware assets (per question 2.0), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1a and provide visibility at the organization's enterprise level?</p>	<p style="text-align: center;">39%</p>

4. Vulnerability Management

<p>4. Provide the number of hardware assets identified in section 2.0 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.</p>	<p style="text-align: center;">185</p>
--	---

**5. Identity and Access Management**

5.1 Provide the number of Organization unprivileged network user accounts? (Exclude privileged network user accounts and non-user accounts)	50	
5.2 How many unprivileged network user accounts are configured to:	5.2a. Require the form of identification listed on the left?	5.2b. Allow, but not require, the form of identification listed on the left?
5.2a (1) (2) User-ID and Password	50	0
5.2b (1) (2) Two factor-PIV Card	0	0
5.2c (1) (2) Other two factor authentication	0	0
5.3 Provide the number of Organization privileged network user accounts (Exclude non-user accounts and unprivileged network user accounts)?	3	
5.4 How many privileged network user accounts are configured to:	5.4a. Require the form of identification listed on the left?	5.4b. Allow, but not require, the form of identification listed on the left?
5.4a (1) (2) User-ID and Password	3	0
5.4b (1) (2) Two factor-PIV Card	0	0
5.4c (1) (2) Other two factor authentication	0	0

6. Data Protection

6. Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table.		
Mobile Assets Types (each asset should be recorded <i>no more than once</i> in each column)	6.a. Estimated number of mobile hardware assets of the types indicated in each row	6.b. Estimated number assets from column a <i>with adequate encryption of data on the device.</i>
6.a(1) / 6.b(1) Laptop Computers, Netbooks, and Tablet-Type Computers	103	100
6.a(2) / 6.b(2) Personal Digital Assistant	0	0
6.a(3) / 6.b(3) BlackBerries and Other Smartphones	42	42
6.a(4) / 6.b(4) USB connected devices (e.g., Flashdrives and Removable Hard Drives)	52	50
6.a(5) / 6.b(5) Other mobile hardware assets	0	0

7. Boundary Protection

7. Provide the percentage of external connections passing through a TIC/MTIPS.	0
--	----------

8. Training and Education

8. Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually).	44
---	-----------

9. Remote Access / Telework

9.1 Provide the estimated total number of annual remote connections the Organization provides to allow users to connect to near-full access to the Organization's normal desktop LAN/WAN resources/services.						5,550
9.1.a For those connections counted above in 9.1, provide the estimated number of those connections that:						
<ul style="list-style-type: none"> REQUIRE the kind (<i>and only the kind</i>) of authentication indicated in 10.1a columns a-d. (List all other connections by connection method in 10.1a column e) For each Type of connection listed below 		9.a-1) ONLY User-ID and Password (KFM)	9.b-2) ONLY Two factor- PIV Card (AP)	9.c-3) ONLY Other two factor authentication	9.d-4) ONLY one other method. (Please describe in the	9.e-5) Connections that may have been authenticated
		5,550	0	0	0	0
Type of Connection	9.a-1a/1b/1c/1d/1e Dial-up	0	0	0	0	0
	9.a-2a/2b/2c/2d/2e Virtual Private Network (<i>not</i> clientless)	5,550	0	0	0	0
	9.a-3a/3b/3c/3d/3e Virtual Private Network (clientless) including SSL, TLS, etc.	0	0	0	0	0
	9.a-4a/4b/4c/4d/4e Citrix	0	0	0	0	0
	9.a-5a/5b/5c/5d/5e Other	0	0	0	0	0