FY 2012
FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

U.S. OFFICE OF GOVERNMENT ETHICS

Prepared by:
Information Resources Management
Office of the Director
November 14, 2012

GENERAL INSTRUCTIONS

Refer to the FY12 CIO Metrics for Definitions pertaining to each section.

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		
FIPS 199 Category	H	M	L	H	M	L	H	M	L
Component 1		/						/	
Component 2									
[Add rows as needed for Organization components]		/						/	

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 (CSP)	
FIPS 199 Category	M	L	M	L	M	L
Component 1		/		/		
Component 2						
[Add rows as needed for Organization components]		/		/		

Purpose and Use

These questions are being asked for the following reasons:

- System inventory is a basic tool to identify systems (and their boundaries).

2. Asset Management		
	2.0 Provide the total number of organization hardware assets connected to the organization's unclassified network(s).	148
	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.	127
	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
	2.4 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
	2.4.a 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 (2.1) on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning.	Yes
3. Configuration Management		
	3.1 For each operating system Vendor, Product, Version, and patch-level combination referenced in 2.2, report the following:	
	3.1a Whether an adequately secure configuration baseline has been defined.	Yes
	3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).	127
	3.1c For what percentage of the applicable	85%

Section 4. Vulnerability Management

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.

OGE does not have any hardware or software utilities that automatically identify NIST vulnerabilities. We procure the IT security services provided by the Bureau of Public Debt to conduct annual reviews of our IT security program. The reviews consist of internal and external vulnerability scanning for NIST vulnerabilities.

Section 5. Identity and Access Management

Provide the number of Organization unprivileged network user accounts? (Exclude privileged network user accounts and non-user accounts.)

5.1 83 network user accounts

How many unprivileged network user accounts are configured to:

	Require the form of ID listed on the left?	**Allow, but not required, the form of ID listed on the left?**
5.2a User-ID and Password	83	0
5.2b Two factor-PIV Card	0	10
5.2c Other two factor Authentication	25	25

Provide the number of Organization privileged network user accounts (Exclude non-user accounts and unprivileged network user accounts)?

5.3 15 network user accounts

How many privileged network user accounts are configured to:

	Require the form of ID listed on the left?	**Allow, but not required, the form of ID listed on the left?**
5.4a User-ID and Password	15	0
5.4b Two factor-PIV Card	0	3
5.4c Other two factor Authentication	25	3

Section 6. Data Protection

Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics.

Enter responses in the table.

Mobile Assists Types	Est. # of mobile hardware assets in each row.	Est # of assets from column A with adequate encryption of data on device.
Laptops, Netbooks & Tablets	87	0
PDA	0	0
BlackBerries/Smartphones	15	0
USB connected devices	100	0
Other	0	0

7. Boundary Protection		
	7. Provide the percentage of external connections passing through a TIC/MTIPS.	100%

Section 8. Training and Education

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

8.0 95%

Section 9. Remote Access/Telework

Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY 2012 (at least annually).

For those connections counted above in 9.1, provide the estimated number of those connections that:

Types of Connection	Kind of Auth.	User/Pass	2 Factor	Other	Possible Auth.
	Dial-up	0	0	0	0
	VPN	2	0	0	0
	SSL VPN	25	25	0	0
	Citrix	0	0	0	0
	Other	25	25	0	0