

Cross Agency Priority Goal

Cybersecurity

Goal Leaders:

Tony Scott, Federal Chief Information Officer;

Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator;

Alejandro Mayorkas, Deputy Secretary, Department of Homeland Security;

Bob Work, Deputy Secretary, Department of Defense



FY2016 Quarter 1

Overview

Goal Statement

Improve awareness of cybersecurity practices, vulnerabilities, and threats to the operating environment by limiting access to authorized users and implementing technologies and processes that reduce risk from malicious activity.

Urgency

The President has identified the cybersecurity threat as one of the most serious national security, public safety, and economic challenges we face as a nation. Ultimately, the cybersecurity challenge in the Federal Government is not just a technology issue. It is an organizational, people, and performance issue requiring creative solutions to address increasingly sophisticated threats and emerging vulnerabilities introduced by rapidly changing technology.

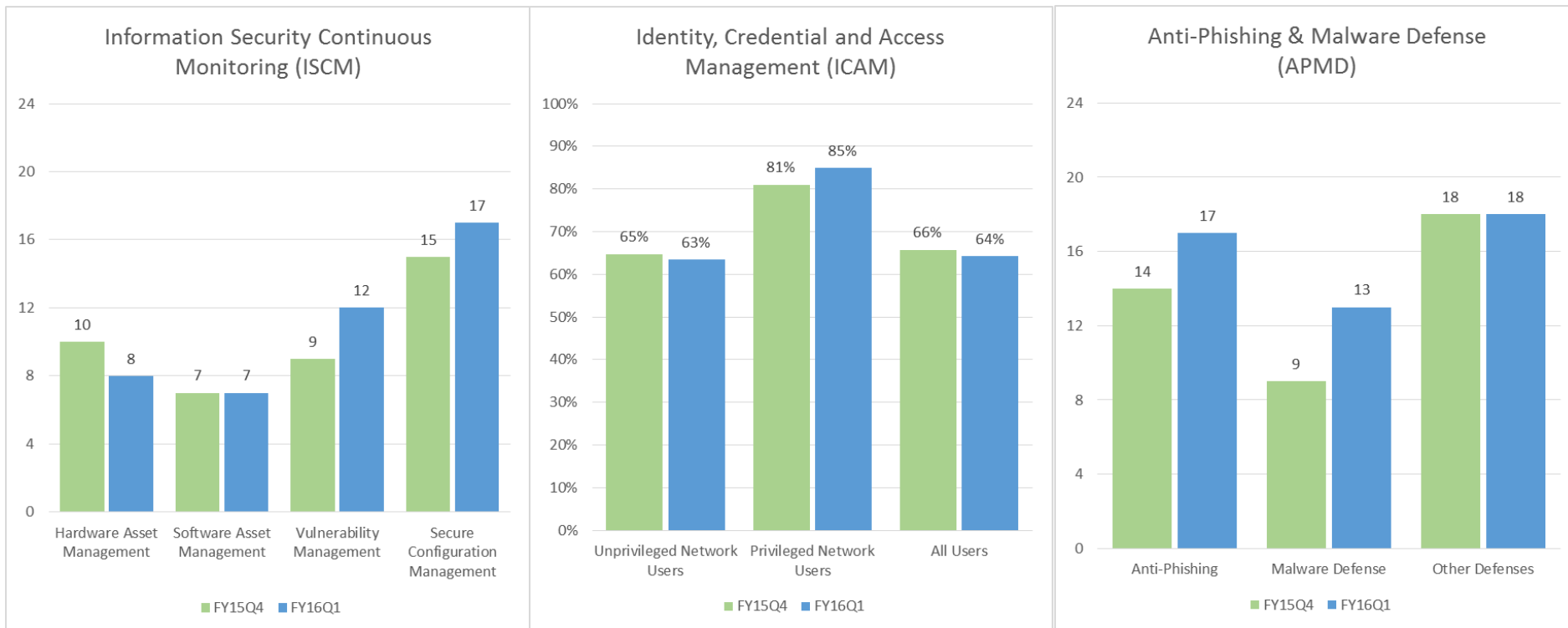
Vision

Implement the Administration's priority cybersecurity capabilities and develop performance-based metrics to measure success. The Administration's FY 2015 – FY 2017 Cybersecurity Cross Agency Priority (CAP) goal is comprised of the following initiatives:

- **Information Security Continuous Monitoring (ISCM)** – Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity.
- **Identity, Credential, and Access Management (ICAM/Strong Authentication)** – Implement a set of capabilities that ensures users must authenticate to information technology resources and have access to only those resources that are required for their job function.
- **Anti-Phishing and Malware Defense (APMD)** – Implement technologies, processes, and training that reduces the risk of malware being introduced through email and malicious or compromised web sites.

Status Update

Civilian CFO Act Agency status toward meeting the Cybersecurity CAP Goal targets in FY 2016 Q1.*



*The number of agencies meeting government-wide targets may vary from quarter to quarter due to fluctuations in the number of information technology assets or number of users at a given agency. This report reflects data from the 23 civilian CFO Act agencies, and therefore excludes information from the Department of Defense and small agencies.

Information Security Continuous Monitoring (ISCM)*

FY 2015 Q4 vs FY 2016 Q1

Hardware Asset Management

Performance must be greater than or equal to 95% for both Hardware Asset Management measures (asset detection, asset meta data collection):

- 8 civilian agencies met both targets in FY 2016 Q1, down from 10 agencies in FY 2015 Q4.

Software Asset Management

Performance must be greater than or equal to 95% for both Software Asset Management measures (software inventory, software whitelisting):

- 7 civilian agencies met both targets in FY 2016 Q1, the same as in FY 2015 Q4.

Vulnerability Management

Performance must be greater than or equal to 95%:

- 12 civilian agencies met the target for FY 2016 Q1, up from 9 agencies in FY 2015 Q4.

Secure Configuration Management

Performance must be greater than or equal to 95%:

- 17 civilian agencies met the target for FY 2016 Q1, the same as in FY 2015 Q4.

Information Security Continuous Monitoring (ISCM)

FY 2015 Q4 vs FY 2016 Q1

Agency	FY 2015 Q4					FY 2016 Q1				
	Hardware Asset Management	Software Asset Management	Vulnerability Management	Secure Configuration Management (SecCM)	ISCM Avg	Hardware Asset Management	Software Asset Management	Vulnerability Management	Secure Configuration Management (SecCM)	ISCM Avg
SSA	100	100	100	100	100	100	100	100	100	100
OPM	100	100	95	99	99	100	100	95	98	98
NRC	100	92	96	99	97	98	95	100	99	98
Labor	99	96	99	100	99	97	97	95	100	97
Justice	97	97	97	99	98	91	99	99	99	97
GSA	73	96	98	95	91	73	97	98	95	91
Treasury	83	91	98	99	93	86	93	99	97	94
USDA	95	100	85	100	95	95	92	85	100	93
HUD	62	0	76	100	60	88	84	100	99	93
DOT	99	90	30	21	60	95	89	70	98	88
State	81	98	82	95	89	81	96	62	95	84
ED	77	17	85	94	68	74	55	100	99	82
NSF	100	0	88	98	72	100	0	91	100	73
Interior	46	57	68	99	68	31	50	95	98	69
SBA	98	2	99	97	74	100	7	100	4	53
VA	0	0	49	99	37	0	2	95	99	49
Commerce	66	72	74	91	76	55	54	77	99	71
EPA	2	67	0	98	42	0	73	1	98	43
DHS	54	58	93	86	73	54	67	93	82	74
HHS	92	32	82	75	70	87	23	84	90	71
USAID	95	0	100	75	68	89	80	0	75	61
Energy	87	39	31	91	62	29	36	66	88	55
NASA	0	2	82	86	43	4	11	91	75	45
Civilian CFO Act Avg	59%	51%	70%	91%		52%	57%	83%	94%	
# Agencies Meeting Targets	10	7	9	15		8	7	12	17	

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 2.2, 2.3, 2.6, 2.7, 2.11, 2.10.6 (FY 2015 Q4) and 1.2, 1.4, 1.5, 2.2, 2.3.1, 2.3.4, 3.16, 3.17 (FY 2016 Q1) from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Civilian CFO Act averages are weighted by the number of hardware assets.

Identity, Credential and Access Management (ICAM)*

FY 2015 Q4 vs FY 2016 Q1

Unprivileged Network Users

Performance must be greater than or equal to 85%.

- Unprivileged user PIV-usage for civilian agencies decreased from 65% in FY 2015 Q4 to 63% in FY 2016 Q1.**
- 18 civilian agencies met the Unprivileged Network Users PIV-usage target in FY 2016 Q1, up from 16 in FY 2015 Q4.

Privileged Network Users

Performance must be equal to 100%.

- Civilian agencies' privileged user PIV-usage increased from 81% in FY 2015 Q4 to 85% in FY 2016 Q1.
- 12 civilian agencies met the Privileged Network Users PIV-usage target in FY 2016 Q1, down from 13 in FY 2015 Q4.

*For more information on the specific ICAM metrics, see the Appendix A - Key Indicators.

**OMB previously reported that the FY 2015 Q4 PIV unprivileged percentage was 81.4% and is restating that percentage in this report to account for civilian CFO Act agencies' reporting an 8% increase in the number of network users in FY 2016 Q1. The significant increase in the number network users that are not currently using PIV cards to log on to agency networks has led to a decrease in the unprivileged user implementation percentage.

OMB is also restating the VA's FY 2015 Q4 PIV implementation percentage for unprivileged users from 80% to 10% to account for VA's expansion of the number of network users that are required to use PIV cards.

Identity, Credential and Access Management (ICAM)

FY 2015 Q4 vs FY 2016 Q1

Agency	FY 2015 Q4			FY 2016 Q1		
	Unprivileged Network Users	Privileged Network Users	All Users	Unprivileged Network Users	Privileged Network Users	All Users
State	38	100	40	100	100	100
OPM	99	100	99	100	100	100
GSA	99	100	99	99	100	99
DOT	97	100	97	98	100	98
Treasury	97	100	97	94	100	94
HUD	95	100	95	93	100	93
NRC	93	97	93	92	100	92
NSF	87	100	88	92	100	92
SBA	89	100	89	91	100	91
EPA	97	100	97	97	98	98
DHS	95	99	95	96	96	96
Labor	92	95	92	95	97	95
Interior	96	100	97	91	98	91
SSA	86	99	87	86	99	87
USDA	86	89	86	85	95	86
HHS	87	99	88	86	90	86
ED	78	27	65	87	79	85
NASA	77	100	77	76	100	77
USAID	35	100	36	37	100	38
VA	10	100	17	10	100	12
Commerce	82	86	82	83	83	83
Justice	64	65	64	64	64	64
Energy	11	7	10	17	17	17
Civilian Avg	65%	81%	66%	63%	85%	64%
DOD	86	51	84	86	51	85
CFO Act Avg	79%	62%	78%	80%	60%	80%

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 3.1.1 and 3.2.1 (FY 2015 Q4) and 2.4, 2.4.1, 2.5, 2.5.1 (FY 2016 Q1) from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Civilian CFO Act averages are weighted by the number of users.

OMB previously reported that the FY 2015 Q4 PIV unprivileged percentage was 81.4% and is restating that percentage in this report to account for civilian CFO Act agencies' reporting an 8% increase in the number of network users in FY 2016 Q1. The significant increase in the number network users that are not currently using PIV cards to log on to agency networks has led to a decrease in the unprivileged user implementation percentage.

OMB is also restating the VA's FY 2015 Q4 PIV implementation percentage for unprivileged users from 80% to 10% to account for VA's expansion of the number of network users that are required to use PIV cards.

Anti-Phishing & Malware Defense (APMD)*

FY 2015 Q4 vs FY 2016 Q1

Anti-Phishing

Performance on Anti-Phishing measures must be greater than or equal to 90% on at least 5 of 7 capabilities:

- 17 civilian agencies met the CAP Goal targets in FY 2016 Q1, up from 14 agencies in FY 2015 Q4.

Malware Defense

Performance on Malware Defense measures must be greater than or equal to 90% on at least 3 of 5 capabilities:

- 13 civilian agencies met the CAP Goal targets in FY 2016 Q1, up from 9 agencies in FY 2015 Q4.

Other Defenses (capabilities related to Anti-Phishing & Malware)

Performance on these measures must be greater than or equal to 90% on at least 2 of 4 capabilities:

- 18 civilian agencies met the CAP Goal targets in FY 2016 Q1, the same as in FY 2015 Q4.

Anti-Phishing & Malware Defense (APMD)

FY 2015 Q4 vs FY 2016 Q1

Agency	FY 2015 Q4			FY 2016 Q1		
	# Capabilities required to have >=90% coverage					
	Anti-Phishing	Malware Defense	Other Defenses	Anti-Phishing	Malware Defense	Other Defenses
	5	3	2	5	3	2
OPM	5	4	3	7	5	4
HUD	6	4	4	7	4	4
Treasury	4	3	4	6	4	4
State	5	4	3	5	5	3
USDA	6	0	2	6	4	3
SSA	6	3	3	5	4	3
DOT	5	3	2	6	3	2
GSA	6	3	2	6	3	2
Labor	6	3	2	5	3	2
NRC	4	2	2	5	3	2
USAID	5	2	3	5	3	2
ED	5	1	0	6	2	2
HHS	5	0	2	6	2	2
Interior	5	2	2	5	2	2
VA	6	2	2	5	1	3
DHS	4	1	2	5	1	2
NSF	5	1	2	5	1	2
SBA	4	1	2	4	4	1
Justice	4	3	1	4	3	1
Commerce	2	1	2	4	0	3
NASA	0	2	0	4	2	1
Energy	3	0	0	3	0	1
EPA	4	0	0	3	1	0
#Agencies meeting targets	14	9	18	17	13	18

Key
Meets or exceeds CAP targets

Source: FISMA Data Agency Level Questions 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 6.1.4, 8.2.1 (FY2015 Q4) and 2.19, 2.19.1, 3.1 through 3.15 (FY2016 Q1) from CyberScope.

Notes: Agencies are sorted by number of CAP Goal targets met

Action Plan Summary

Initiative*	Major Actions to Achieve Impact	Key Indicator/Targets for FY 2015 Q3 thru FY 2017
Information Security Continuous Monitoring (ISCM)	<ul style="list-style-type: none"> Understand the hardware and software on Federal networks and the risks that they pose; and Maintain ongoing, near real-time awareness of information security risks and have the capability to rapidly respond to support organizational risk management decisions. 	<ul style="list-style-type: none"> Hardware Asset Management: Detection of devices or device hardware characteristics must be greater than or equal 95%. Software Asset Management: Detection of software inventory or base level application configurations (whitelisting) must be greater than or equal 95%. Vulnerability Management: Detection of hardware or software vulnerabilities must be greater than or equal 95%. Secure Configuration Management: Validation of select OS software configurations must be greater than or equal 95%.
Identity, Credential, and Access Management (ICAM/ Strong Authentication)	<ul style="list-style-type: none"> Ensure only authorized users have access to Federal information systems; and Ensure only authorized users have access to information needed for designated business functions. 	<ul style="list-style-type: none"> Unprivileged Network Users: Unprivileged users required to use PIV for network log-on must be greater or equal to 85%. Privileged Network Users: Privileged users required to use PIV for network log-on must be equal to 100%.
Anti-Phishing & Malware Defense (APMD)	<ul style="list-style-type: none"> Implement technologies, processes, and training to reduce the risk of malware introduced through email and malicious or compromised web sites. 	<ul style="list-style-type: none"> Anti-Phishing: 5 of 7 capabilities with anti-phishing toolsets must be greater than or equal to 90%. Malware Defense: 3 of 5 capabilities with malware toolsets must be greater than or equal to 90%. Other Defense (capabilities related to Anti-Phishing & Malware): 2 of 4 capabilities with a blended toolset must be greater than or equal to 90%.

* The corresponding indicators for these CAP Initiatives are captured in the Key Indicators section of this report.

Work Plan

Milestone Summary			
Key Milestones	Milestone Date	Milestone Status	Issues / Comments
OMB FY 2015 – FY 2016 FISMA reporting guidance released	10/30/15	Complete	http://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf
FY 2016 CIO FISMA/CAP metrics published	10/30/15	Complete	http://www.dhs.gov/publication/fy16-fisma-documents
FY 2015 FISMA annual/Q4 metrics reports due	11/13/15	Complete	https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf
FY 2016 Q1 CAP metrics updates due	1/15/16	Complete	
FY 2016 Q2 CAP metrics updates due	04/15/16		
FY 2016 Q3 CAP metrics updates due	07/15/16		
FY 2016 Annual/Q4 CAP metrics updates due	11/10/16		Also known as the FY 2016 FISMA annual report due date

Appendix A - Key Indicators

CAP Initiatives	Area	Question No.	Question
Information Security and Continuous Monitoring	Hardware Asset Management	1.2	Number of the organization's hardware assets connected to the organization's unclassified network(s).
		1.4	Number of GFE hardware assets (from 1.2.) covered by an automatic (e.g. scans/device discovery processes) hardware asset inventory capability at the enterprise-level. (CAP)
		3.16	Percent (%) of the organization's unclassified network that has implemented a technology solution to detect and alert on the connection of unauthorized hardware assets. (CAP)
	Software Asset Management	1.2.1	Percent (%) of endpoints from 1.1.1 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll).
		1.2.2	Percent (%) of endpoints from 1.1.1 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g. AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).
		1.5	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by an automated software asset inventory capability at the enterprise-level. (CAP)
		3.17	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions). (CAP)
	Vulnerability Management	2.2	Percent (%) of the organization's unclassified network(s) assessed for vulnerabilities using Security Content Automation Protocol (SCAP) validated products ³ . (CAP)
	Secure Configuration Management	2.3.1	Number of hardware assets with each OS. (Base)
		2.3.4	Number of assets in 2.3.1 covered by auditing for compliance with 2.3.2. (CAP)

Appendix A - Key Indicators (cont.)

CAP Initiatives	Area	Question No.	Question
Identity Credential and Access Management	Unprivileged users	2.4	Number of users with unprivileged network accounts. ⁴ (Exclude privileged network accounts and non-user accounts.) (Base)
		2.4.1	Number of users (from 2.4.) technically required to log onto the network with a two-factor PIV card ⁵ or NIST Level of Assurance (LOA) 4 credential. ⁶ (CAP)
	Privileged users	2.5	Number of users with privileged network accounts. (Exclude unprivileged network accounts and non-user accounts.) (Base)
		2.5.1	Number of users (from 2.5.) technically required to log onto the network with a two-factor PIV card ⁷ or NIST LOA 4 credential. (CAP)
Anti-Phishing & Malware Defense	Anti-Phishing	2.19	Number of users that participated in exercises focusing on phishing that are designed to increase awareness and/or measure effectiveness of training, (e.g. organization conducts spoofed phishing emails, clicking links leading to phishing information page). (Base)
		2.19.1	Number of users (from 2.19.) that successfully passed the exercise. (CAP)
		3.1	Percent (%) of incoming email traffic passing through anti-phishing and anti-spam filtration at the outermost border mail agent or server. (CAP)
		3.2	Percent (%) of incoming email traffic analyzed using sender authentication protocols (e.g., DKIM, ADSP, DMARC, VBR, SPF, iprev). (CAP)
		3.3	Percent (%) of incoming email traffic analyzed using a reputation filter (to perform threat assessment of sender). (CAP)
		3.4	Percent (%) of incoming email traffic analyzed for detection of clickable URLs, embedded content, and attachments. (CAP)
		3.5	Percent (%) of incoming email traffic analyzed for suspicious or potentially nefarious attachments opened in a sandboxed environment or detonation chamber. (CAP)
		3.6	Percent (%) of outgoing email traffic that enables the recipients to verify the originator using sender authentication protocols (e.g., DKIM, ADSP, DMARC, VBR, SPF, iprev). (CAP)

Appendix A - Key Indicators (cont.)

CAP Initiatives	Area	Question No.	Question
Anti-Phishing & Malware Defense	Malware Defense	3.7	Number of GFE endpoints (from 1.2.1.) covered by an intrusion prevention system. (CAP)
		3.8	Number of GFE endpoints (from 1.2.1.) covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information. (CAP)
		3.9	Number of GFE endpoints (from 1.2.1.) covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (CAP)
		3.10	Number of GFE endpoints (from 1.2.1.) protected by a browser-based (e.g., Microsoft SmartScreen Filter, Microsoft Phishing Filter, etc.) or enterprise-based tool to block known phishing websites and IP addresses. (CAP)
		3.11	Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) authorized for remote access connection to the unclassified network. (Base)
		3.11.1	Number of assets (from 3.11.) scanned for malware prior to an authorized remote access connection to the unclassified network. (CAP)
	Other Defenses (capabilities related to Anti-Phishing & Malware)	3.12	Percent (%) of privileged user network accounts (from 2.5.) that have a technical control limiting access to only trusted sites. (CAP)
		3.13	Percent (%) of inbound network traffic that passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers). (CAP)
		3.14	Percent (%) of outbound communications traffic checked at the external boundaries to detect encrypted exfiltration of information (i.e. D/A's capability to decrypt/interrogate and re-encrypt). (CAP)
		3.15	Percent (%) of email messages processed by systems that quarantine or otherwise block suspected malicious traffic. (CAP)

Acronyms

APMD	Anti-Phishing and Malware Defense
CAP	Cross Agency Priority
CFO	Chief Financial Officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOT	Department of Transportation
ED	Department of Education
Energy	Department of Energy
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
ICAM	Identity, Credential, and Access Management
Interior	Department of the Interior
ISCM	Information Security Continuous Monitoring
Justice	Department of Justice
Labor	Department of Labor
NASA	National Aeronautics and Space Administration
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OPM	Office of Personnel Management
PIV	Personal Identity Verification
SBA	Small Business Association
SSA	Social Security Administration
State	Department of State
Treasury	Department of the Treasury
USAID	United States Agency for International Development
USDA	Department of Agriculture
VA	Department of Veterans Affairs