

Cross Agency Priority Goal: Cybersecurity

FY2013 Q1 Status Update

Cross Agency Priority Goal Statement

Executive branch departments and agencies will achieve 95% implementation of the Administration's priority cybersecurity capabilities by the end of FY 2014. These capabilities include strong authentication, Trusted Internet Connections (TIC), and Continuous Monitoring.

Goal Leader

J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator

About this document

The Cross-Agency Priority (CAP) Goals were a key innovation introduced in the FY2013 Federal Budget. These goals focus on 14 major issues that run across several Federal agencies. Each of these historic goals has a Goal Leader who is a senior level White House official and is fully accountable for the success and outcomes of the goal.

Historically, areas of shared responsibility for multiple government agencies have been resistant to real progress. Success in these areas requires a new kind of management approach – one that brings people together from across and outside the Federal Government to coordinate their work and combine their skills, insights, and resources. The CAP Goals represent Presidential priorities for which this approach is likeliest to bear fruit.

This report discusses one of these CAP Goals, the Cybersecurity Goal, in detail, describing the plan for achieving the goal and the current status of progress. To see the full list of CAP Goals and to find out more about them, we encourage you to visit performance.gov.

Contents

Cross Agency Priority Goal Statement	1
Goal Leader	1
Overview	3
Strategies and Action Plan	3
Use the FISMA Governance Structure	4
Embrace Federal Information Security Management Principles	4
Cross-Agency Coordination.....	5
Deputy Secretary Coordination	5
Performance Improvement Officer (PIO)/Chief Financial Officer (CFO) Coordination	5
Chief Information Officer (CIO)/Chief Information Security Officer (CISO) Coordination.....	6
National Security Systems Coordination.....	6
Monitoring and Reviewing Progress.....	6
1. Longer-term Milestones	7
2. Milestones for the Upcoming Quarter (FY2013 Q2).....	8
3. Contributing Programs and Other Factors.....	10
Progress Update.....	13
Scorecards.....	16
Key Indicators and Metrics	21
Milestones Accomplished to Date (FY13Q1)	22

Overview

The Federal cybersecurity Cross-Agency Priority Goal helps Federal departments and agencies improve cybersecurity performance by focusing efforts on *what data and information is entering and exiting their networks, what components are on their information networks and when their security status changes, and who is on their systems*. The White House will focus agency efforts on improving the security of their networks by implementing the Administration's priority cybersecurity capabilities and developing metrics to measure their success. The Administration's priority cybersecurity capabilities are:

- Trusted Internet Connections (TIC) - Consolidate external Internet traffic and ensure a set of common security capabilities for situational awareness and enhanced monitoring.
- Continuous Monitoring of Federal Information Systems - Transform the historically static security control assessment and authorization process into an integral part of a dynamic enterprise-wide risk management process. This change allows departments and agencies to maintain an ongoing near-real-time awareness and assessment of information security risk and rapidly respond to support organizational risk management decisions.
- Strong Authentication – Ensure only authorized employees have access to Federal information systems by requiring a higher level of assurance following the HSPD-12 Personal Identity Verification standard.

Strategies and Action Plan

The Cybersecurity CAP Goal strategy is to help Federal departments and agencies improve cybersecurity performance so they can provide secure and effective services to the American people. Federal departments and agencies need to focus their cybersecurity activity on the most cost-effective and efficient cybersecurity controls relevant for Federal information system security.

Therefore, the Cybersecurity CAP goal strategy starts with holding agency leadership accountable for Cybersecurity. The Deputy Secretary for each agency is responsible with leading their organization's efforts to implement the Administration's priority cybersecurity capabilities. The Performance Improvement Officer (PIO), frequently the same person as the Chief Financial Officer (CFO), is

Effective leadership anchored at the White House alone will not be sufficient to achieve the broad range of objectives necessary to lead the United States in the digital age. Leadership and accountability must extend throughout the Federal government.
Cyberspace Policy Review – May 2009

responsible for improving the performance of their department or agency programs, including Cybersecurity performance. An empowered Chief Information Officer (CIO) with executive leadership support, authority and resources to direct agency activity is necessary to successfully implement these priorities and report agency progress to the Deputy Secretary.

Implementation should be coordinated across multiple stakeholders, including cross-agency coordination using established bodies such as the President’s Management Council (PMC), the Performance Improvement Council (PIC), and the CIO Council.

Finally, these priority capabilities should be included in agency strategic plans, budget submissions, and annual performance plans.

Use the FISMA Governance Structure

The Cybersecurity Cross Agency Priority (CAP) Goal uses the Federal Information Security Management Act (FISMA) of 2002 reporting structure, guidelines and metrics to measure agency progress. FISMA requires agencies to provide information security protections commensurate with risks and their potential harms to governmental information systems, to review their information security program, and to report results to the Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with the act.

OMB Memorandum 10-28 “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President (EOP) and the Department of Homeland Security (DHS)” designated DHS to exercise primary responsibility within the Executive Branch for the operational aspects of Federal department and agency cybersecurity initiatives with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543. OMB requires departments and agencies to adhere to DHS direction for reporting data on the security status of their information systems through the DHS CyberScope reporting tool.

Embrace Federal Information Security Management Principles

The Administration’s priority cybersecurity capabilities and the Cybersecurity CAP goal embrace three principles for good Federal information security management:

- **Accountability with standard milestones** – Department and agency progress on the Cybersecurity CAP Goal is measured quarterly and annually through the FISMA reporting process. Agencies and components are held accountable to leadership and the public through increased visibility and reporting frequency. Regular progress reporting occurs through manual and automated data feeds that are reported to

OMB, DHS, and agency leadership, including the Deputy Secretary and Performance Improvement Officer.

- Agencies are encouraged to highlight their progress towards the Administration's priority cybersecurity capabilities through additional descriptions of specific activities that may not be captured in a reportable FISMA metric. Additionally, agencies are encouraged to highlight for senior leadership review any impediments that reduce or restrict progress on implementing these priority capabilities, especially if agencies do not expect to meet their planned cybersecurity capability targets.
- **Visibility through automation** - Adopt automated reporting standards for continuous monitoring to increase visibility and sharing of agency cybersecurity posture. Enhanced visibility of the current security status and threats to the Federal IT environment provides greater situational awareness to improve defense and response.
- **Mature information security management measurement** – It is hard to measure good cybersecurity, so the Federal government is focusing on improving cybersecurity performance by evolving from checklist audits to outcome-based maturity metrics for department and agency information security management.

Cross-Agency Coordination

The Administration's priority cybersecurity capabilities require cross-agency coordination using established bodies:

Deputy Secretary Coordination

- **President's Management Council (PMC):** The PMC provides performance and management leadership throughout the executive branch of the Federal Government and advises and assists the President on government reform. The PMC is focused on identifying and adopting cross-cutting best practices government-wide and working with the other Councils to streamline policy development and facilitate cost savings.

Performance Improvement Officer (PIO)/Chief Financial Officer (CFO) Coordination

- **Performance Improvement Council (PIC):** The PIC is composed of the Performance Improvement Officers (PIOs) of Federal agencies and departments and senior OMB officials. The PIC collaborates to improve the performance of Federal programs and facilitates information exchange among agencies. The PIC provides support to Federal Government PIOs and other program officials to facilitate coordination on cross-cutting performance areas, to include work in support of Federal Priority Goals.

Chief Information Officer (CIO)/Chief Information Security Officer (CISO) Coordination

- **Federal CIO Council:** The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources and is led by the Federal CIO.
 - **Information Security and Identity Management Committee (ISIMC) -** ISIMC manages high-priority security and identity management initiatives and develops recommendations for policies, procedures, and standards to address those initiatives.

National Security Systems Coordination

- **The Committee on National Security Systems (CNSS):** The CNSS provides a forum for the discussion of policy issues, and is responsible for setting national-level information assurance policies, directives, instructions, operational procedures, guidance, and advisories for departments and agencies for the security of National Security Systems through the CNSS Issuance System. CNSS promotes collaboration on cybersecurity efforts among owners of Federal National Security Systems, Federal non-National Security Systems, and non-Federal systems.

Monitoring and Reviewing Progress

As specified under FISMA, all Federal information systems must follow prescribed information security standards and reporting guidance. The Cybersecurity CAP Goal applies to all Federal information systems that fall under the FISMA framework for compliance, oversight, and reporting. This includes both non-national security systems and National Security Systems.

Department and agency progress towards the Cybersecurity CAP Goal follows the same monthly and quarterly FISMA reporting requirements as specified by OMB¹ and the same FISMA metrics and operational guidance provided by DHS.

Progress reporting should be no less than quarterly as required under GPRA Modernization.² As Federal agencies transition to continuous monitoring, this frequency should increase as defined by the DHS continuous monitoring program. Agency progress towards milestones will use the DHS FISMA reporting process to report progress on the

¹ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf>

² As stated in the GPRA Modernization Act of 2010 Sec. 1121. *Quarterly priority progress reviews and use of performance information*, the cybersecurity CAP Goal progress will be reviewed to assess whether agencies are making progress towards milestones as planned.

Administration’s priority cybersecurity capabilities. Whenever possible, reporting on the CAP milestones should use an automated reporting system.

NSS and OMB will schedule a CyberStat meeting or other appropriate action for those agencies at risk of not achieving the planned level of cybersecurity capability performance. Such meetings will focus on identifying prospects and strategies to improve cybersecurity performance. DHS facilitates the CyberStat process, and it will document performance improvement plans, follow up with each department or agency at risk, and report progress back to the Cybersecurity CAP Goal leadership.

1. Longer-term Milestones

Milestone
All Deputy Secretaries meet at least annually with PIOs and CIOs to review Cybersecurity CAP goal progress.
All PIOs and CIOs meet at least quarterly to review Cybersecurity CAP goal progress.
All departments and agencies report continuous diagnostics data to DHS and DHS integrates to reporting dashboard.
All Departments and Agencies meet the OMB requirements for ongoing authorization through continuously monitoring security controls.
All Departments and Agencies support at least 90% of employees to have the option to use Personal Identity Verification (PIV) Card to authenticate.
All PIOs and CIOs send a PIV-signed email to DHS to validate they have their PIV card, reader, and software.
All CIOs use mandatory PIV authentication by end of FY13.
ISIMC, CNSS, and other interagency working groups propose recommendations to align information security initiatives between national and non-national security systems.
The Joint Continuous Monitoring Working Group provides guidance for the provisional frequency of and activities associated with monitoring the security controls from National Institute of Standards and Technology (NIST) SP 800-53 and CNSSI 1253 baselines to support the OMB requirements for ongoing authorization.
DHS rolls out a federal-wide continuous diagnostics program over the next three-years.
DHS collects all cybersecurity priority metrics through automated reporting mechanisms.
DHS proposes a risk-based framework for addressing the maturity of continuous monitoring capabilities including the effectiveness of security controls and progressive improvement of FISMA implementation.
DHS updates TIC program to support cloud computing and mobile technology.
DHS works with NIST and General Services Administration (GSA) to develop lower cost Managed Trusted Internet Protocol Services (MTIPS) alternatives using new scoring criteria.
NIST releases final version of FIPS 201-2 and related PIV documentation.
FedRAMP obtains Joint Authorization Board provisional Authorizations to Operate for Cloud Service Providers.

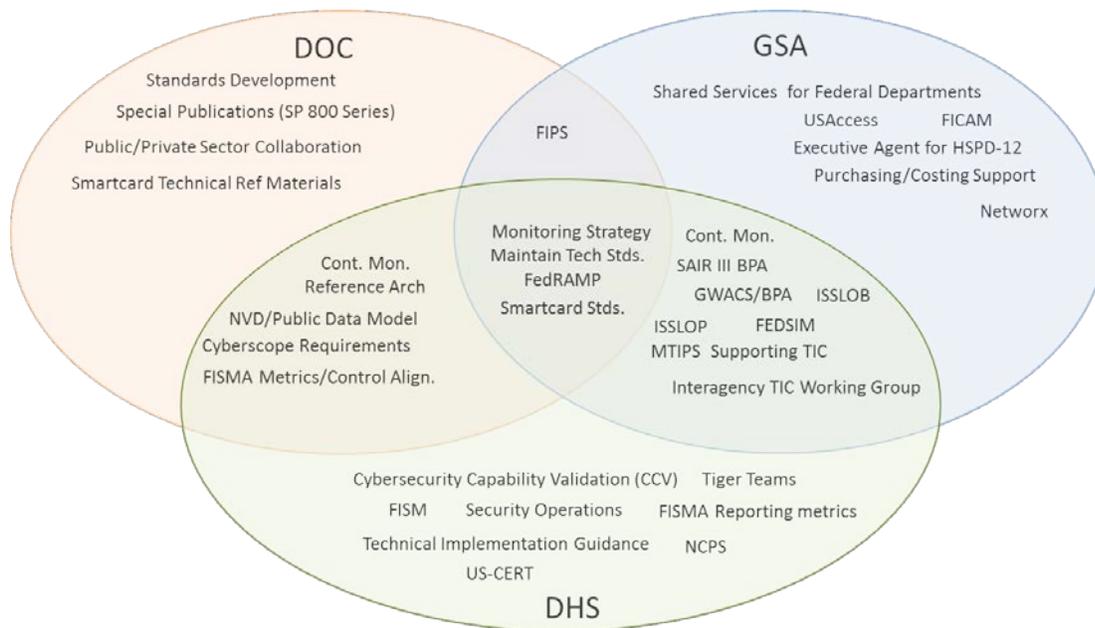
2. Milestones for the Upcoming Quarter (FY2013 Q2)

Milestone	Status
Q2FY13: DHS and NIST sign formal Memorandum of Agreement for coordination on Continuous Monitoring.	Completed
Q2FY13: NIST: Finalize NIST Interagency Report 7511 Rev. 3. Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements. This defines the requirements that must be met by products to achieve SCAP 1.2 Validation. Validation is awarded based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program.	Completed
January 4 & February 19, 2013: DHS to update the Federal stakeholders on the DHS Continuous Monitoring and Diagnostics (CDM) program status.	Completed
March 31, 2013: NIST: Post SP 800-63-2 for public comment. This recommendation provides technical guidelines for Federal agencies implementing electronic authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks.	Completed
March 31, 2013: GSA will develop, in consultation with DHS and NIST, an education and awareness document focused on communicating the value of PIV card usage.	
<p>March 31, 2013: GSA and DHS, working through the CXO Councils, will charter one or more tiger teams focusing on the implementation of OMB M-11-11 for strong authentication to networks and information systems, comprised of participants from CFO Act agencies, to:</p> <ul style="list-style-type: none"> • Develop a PIV Logical Access Control System (LACS) business case • Develop a methodology and conduct PIV LACS-related cost and savings analysis • Collect and evaluate D/A policies and implementing processes related to PIV LACS and develop policy recommendations • Identify USG-enterprise systems and/or websites for priority consideration/decision to PIV-enable and mandate PIV usage. • Develop standard language for use by requiring officials in acquisitions to support PIV enablement and PIV compatibility and interoperability • Evaluate the need for new procurement policy and/or guidance and, if needed, provide policy recommendations to GSA and OMB • Identify existing procurement vehicles and investigating new vehicles to provide PIV LACS Technical Support with input from the SLATT needs assessment. 	
March 31, 2013: GSA and NIST to develop a “solutions to PIV implementation barriers” document for D/As to accelerate prioritization and implementation of PIV mandatory authentication.	

March 31, 2013: GSA, in coordination with DHS and DOC, will coordinate with the Strategic Sourcing Cross Agency Priority Goal on a roadmap of deliverables to identify commodity IT services and solutions supporting the implementation of the Administration's priority cybersecurity capabilities.	
March 31, 2013: NIST to develop a plan to work with solution providers to increase in the number and diversity of devices that support mandatory PIV authentication in use across the USG.	
March 31, 2013: DHS, in coordination with the Joint Continuous Monitoring Working Group (JCMWG), define program implementation responsibilities.	
March 31, 2013: DHS, in coordination with the JCMWG, develop a near, mid, and long term CDM deployment roadmap, with specific deployment milestones and actions of CDM capabilities.	
March 31, 2013: DHS to perform at least three CyberStats, focusing specifically on PIV LACS mandatory authentication performance	
March 31, 2013: DHS to develop a Federal Network Resilience (FNR) Risk Assessment Process overview document describing how FISMA data collected is used by NCCIC/USCERT and other D/As for risk analysis and assessment.	
March 31, 2013: DHS will collect performance plans and measure performance to see if D/As will hit their targets.	

3. Contributing Programs and Other Factors

The mission areas of the three contributing agencies (DHS, Department of Commerce, and GSA) provide support activities that enable other Federal departments and agencies to implement the Administration’s priority cybersecurity capabilities. These include the DHS National Cyber Security Division (NCSD), the DOC, NIST and the GSA Office of Citizen Services and Innovative Technologies (OCSIT), Office of Government-wide Policy (OGP), and Federal Acquisition Service (FAS).



The FY2011 FISMA program introduced the Administration’s priority cybersecurity capabilities and reported progress through the FY2011 FISMA report³, and continued with the FY2012 and FY2013 FISMA metrics⁴.

FISMA minimal and target levels apply to each individual Federal department or agency, as reported through Cyberscope. The Cybersecurity CAP Goal measures cross-agency performance across all U.S. Government Federal executive branch departments and agencies. Table 1 estimates government-wide performance to targets based on the FY2012 FISMA data. In certain cases cybersecurity CAP Goal progress will accommodate classified or aggregated reporting, such as described under FISMA for national security systems reporting.

	CAP - Actual		CAP (All USG) - Projected								FISMA (D/A)	
	FY2012Q4	FY2013Q1	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q4	FY2014Q1	FY2014Q2	FY2014Q3	FY2014Q4	Min	Target
Continuous Monitoring ⁵	79.53%	78.42%	81.46%	83.40%	85.33%	87.27%	89.20%	91.13%	93.07%	95.00%	80.00%	95.00%
Strong Authentication	57.26%	53.72%	61.35%	65.45%	69.54%	73.63%	77.72%	81.82%	85.91%	90.00%	50.00%	75.00%
TIC Consolidation	81.22%	84.00%	82.94%	84.67%	86.39%	88.11%	89.83%	91.56%	93.28%	95.00%	80.00%	95.00%
TIC Capabilities	83.87%	82.21%	85.89%	87.90%	89.92%	91.94%	93.95%	95.97%	97.98%	100.00%	95.00%	100.00%
Cyber CAP	76.82%	75.87%	79.10%	81.37%	83.64%	85.91%	88.18%	90.46%	92.73%	95.00%	NA	NA

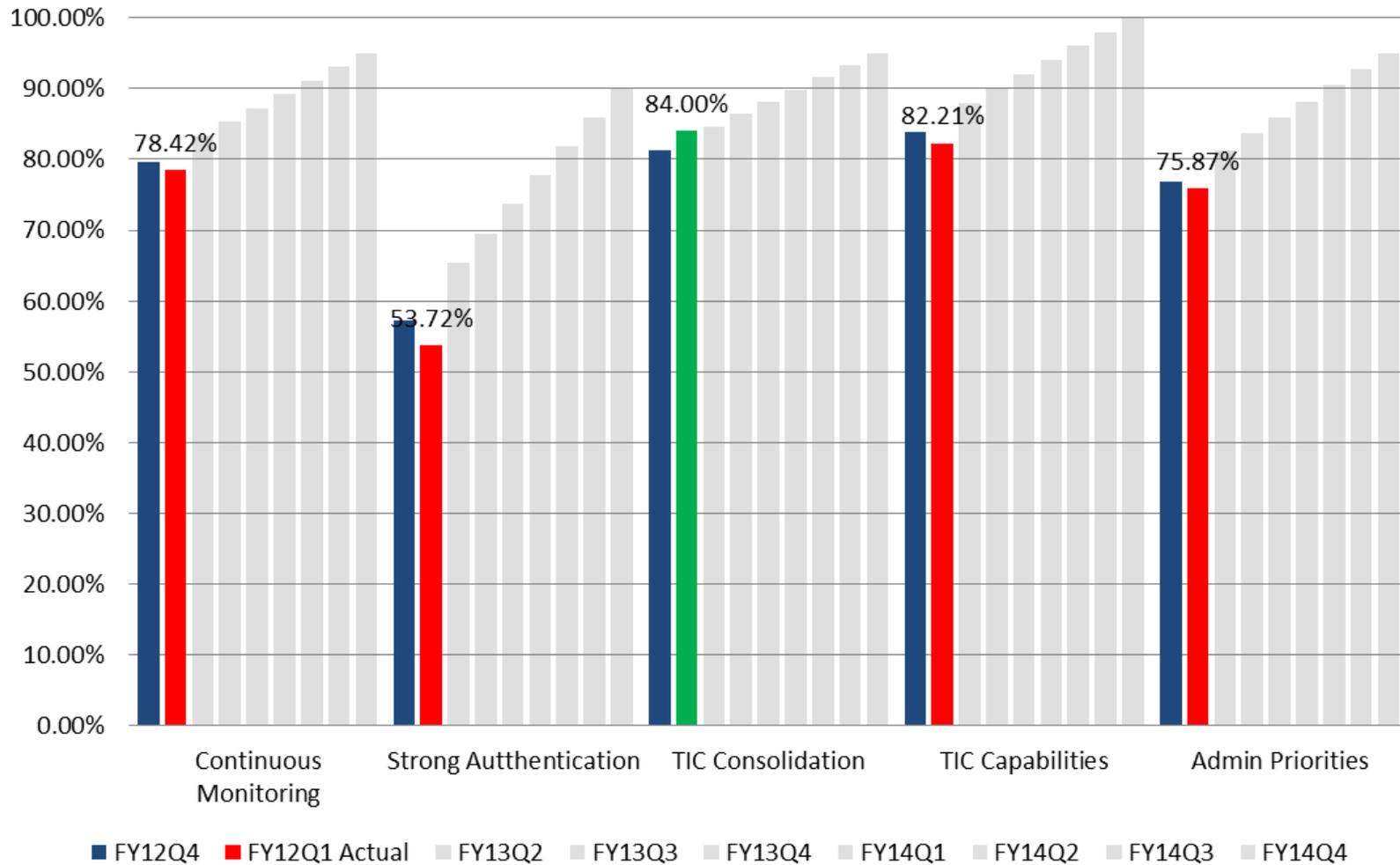
Table 1: Cybersecurity CAP Quarterly targets

³ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_e-gov_act_report.pdf

⁴ <http://www.dhs.gov/xlibrary/assets/nppd/ciofismametricsfinal.pdf>

⁵ Continuous Monitoring is weighted as it is the average of continuous monitoring asset, configuration, and vulnerability scores.

Administration's Priority Cybersecurity Capabilities



Progress Update

Based on the Q1 FY2013 Cyberscope reports on the Administration's priority cybersecurity capabilities, agencies have made substantial progress against the Cybersecurity Cross Agency Priority (CAP) goal. Despite the drop in overall CAP score, much of it associated with adjustments and improvements to measurement methodology, the data reflect continued agency attention to the priority capabilities. At the same time, we are working to accelerate progress on the Cybersecurity CAP Goal. The chart below represents the results of the annual FY2012 and Q1 FY2013 FISMA reporting for the Administration's priority cybersecurity capabilities.

	USG-Wide FISMA Results		USG-Wide CAP Target	
	FY2012 Q4	FY2013 Q1	Min FY2012	Target FY2014
Continuous Monitoring	79.53%	78.42%	80%	95%
Strong Authentication	57.26%	53.72%	50%	90%
TIC Consolidation	81.22%	84.00%	80%	95%
TIC Capabilities	83.87%	82.21%	95%	100%
Weighted Average	76.82%	75.87%	77.50%	95%

FISMA Metrics

To have meaningful measurement of progress over time the FISMA metrics must remain reasonably consistent in the security capabilities they measure. While evaluating implementation improvement requires consistency, the metrics must also be flexible enough to include additional threat vectors. From FY2012 to FY2013 there was a slight shift in the factors determining two of the Administration's priority cybersecurity capabilities, although the focus remained the same.

Based on the recommendations of the Strong Logical Access Tiger Team (SLATT), the Strong Authentication metric changed in FY2013 to address people rather than just accounts. This metric now includes requiring two-factor PIV authentication for people logging on remotely. As the Federal Government promotes telework and increases their mobile workforce, remote access to network resources must require strong authentication mechanisms.

The TIC Capabilities metric advanced from version 1.0 to version 2.0. TIC v2.0 updates the TIC baseline security capabilities in the TIC architecture, based on evolving and increasingly sophisticated threats. It deploys EINSTEIN 2, an Intrusion Detection System (IDS) capability that alerts when a specific cyber threat is detected, and other network changes needed to support Internet Protocol version 6 (IPv6). TIC capability scores dropped slightly as federal agencies move from the 51 security requirements of TIC 1.0 to the 76 requirements of TIC 2.0.

FY2013 Q1 FISMA reporting through CyberScope erroneously omitted data necessary for computing the Cybersecurity CAP Goal quarterly progress report for Configuration Management, under the Continuous Monitoring priority capability. Unlike previous quarterly reports, CyberScope did not collect the total number of applicable assets with configuration management software. DHS sent a supplemental data call to capture the total number of assets under configuration management. For agencies that did not respond to this data call with FY2013 Q1 data, DHS used FY2012 Q4 data to calculate configuration management.

FY2013 Q1 Summary

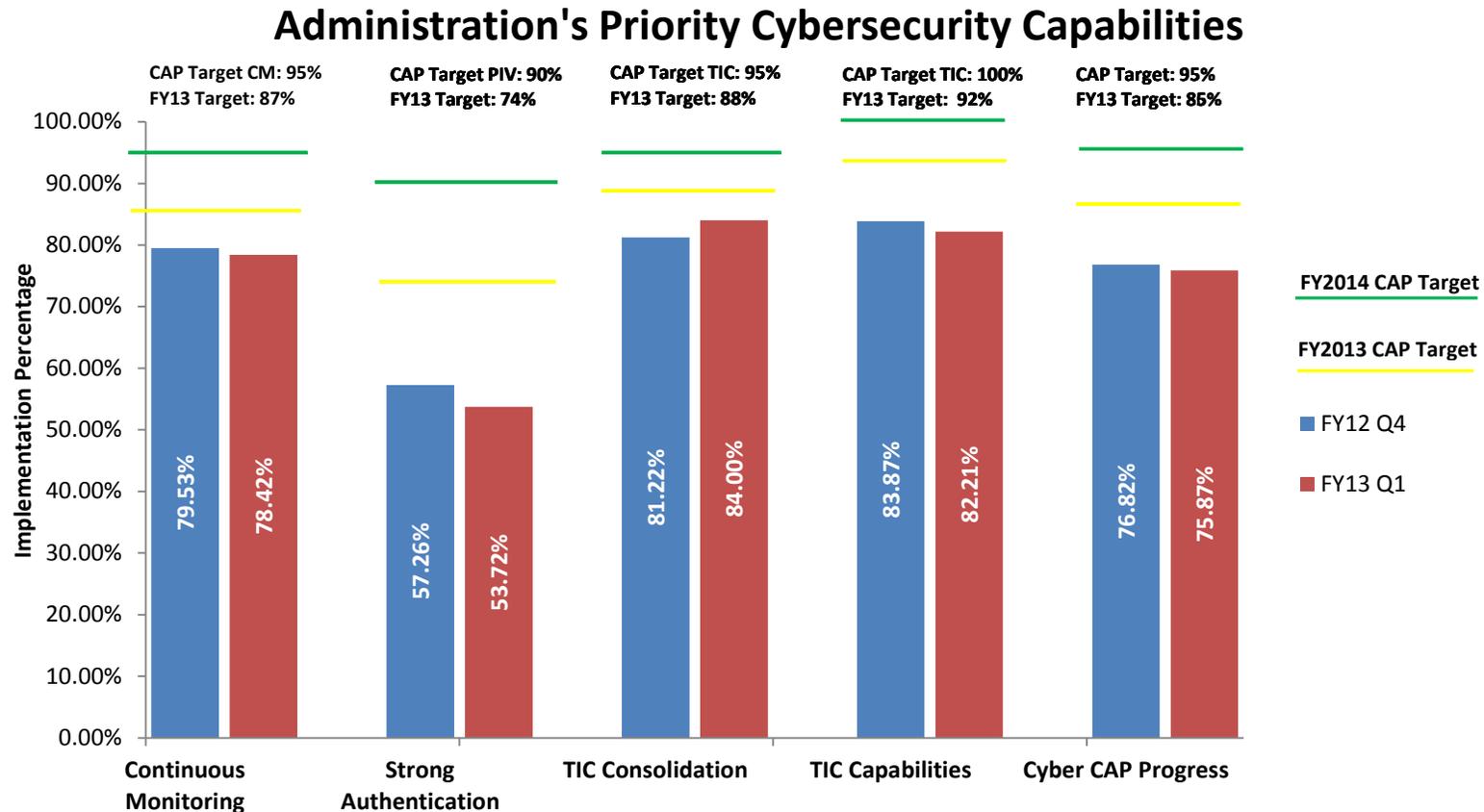
- The overall Cyber CAP score decreased by 0.95% from FY12 Q4 to FY13 Q1 due to a shift to new metrics and TIC 2.0 architecture from FY12 to FY13. The new metrics and architecture establish the baseline for the two-year Cyber CAP Goal.
 - The overall Continuous Monitoring score decreased by 1.11%, as new metrics provided increased fidelity for asset discovery and management, and increased detailed reporting for configuration management.
 - TIC Consolidation increased by 2.78% while TIC Capabilities decreased by 1.66% as agencies moved from the TIC 1.0 to the TIC 2.0 architecture, which added an additional 25 security capability requirements.
 - Strong Authentication decreased 3.54%, due to new metrics for strong authentication as recommended by a 2012 interagency Tiger Team. The recommendations of this team included focusing on strong authentication using HSPD-12 cards of persons rather than accounts, which incorporated new metrics for privileged users and remote access.
- Continuous Monitoring
 - Eighteen agencies reached the minimum target for Automated Asset Management of 80%, and twelve reached the FY13 target of 95%. Government-wide, automated asset management increased by 2.74%
 - Half the agencies remained flat for Automated Vulnerability Management but the government-wide average decreased due to a third of agencies reporting decreases.
 - Automated Configuration Management decreased by 4% in FY13Q1. Not all agencies reported for this quarter, in which case the CAP goal metric used FY12Q4 reported data.
- Strong Authentication
 - In FY13, the use of PIV cards for Remote Access was included in the calculation of this measure. This caused significant swings, both up and down, in the PIV scores of several agencies.
 - The inclusion of Remote Access PIV was a significant portion of the increase in PIV scores for DOI, OPM, SSA, and State.

- The inclusion of Remote Access PIV caused a significant decrease in PIV scores for EDU.
- DOE, DOI, DOJ, NASA, OPM, Treasury, and SSA are no longer at 0% as they implemented some degree of mandatory PIV cards for network access.
- Half the agencies have 2% or less PIV implementation, with a full third still at 0%.
- DOD and GSA are currently the only agencies reporting at or above the FY2013 target.
- Trusted Internet Connection (TIC)
 - Nineteen agencies achieved the minimum FY13 FISMA target of 80% consolidation and fifteen of these have achieved the goal of 95% or greater TIC Traffic Consolidation. GSA, HHS, VA and DOE have not yet met the minimum target for TIC Consolidation.
 - Most agencies remained relatively stable on TIC capabilities, with no agency showing any major decrease. At the same time, several agencies made noteworthy progress:
 - DOJ and USAID achieved the minimum capabilities for TIC 2.0
 - NRC and Treasury achieved full implementation of TIC 2.0 capabilities.
 - Agencies using MTIPS vendors are not responsible for reporting their TIC Capability score, because MTIPS inherently provides this capability. This included DOL, GSA, NSF, and SBA.

Scorecards

The graphs below represent two types of scorecards. The first shows government-wide performance towards the Administration's Priority Cybersecurity Capabilities. The FY2013 FISMA metrics provides more details on the calculation of the government-wide score. The remaining scorecards show individual Federal department and agency performance towards the Administration's Priority Cybersecurity Capabilities. Note the FY2013 FISMA targets are different from the government-wide CAP targets for FY2014.

Government-wide performance towards the Administration's Priority Cybersecurity Capabilities as of FY13 Q1



The Cyber CAP Progress is an overall measure that combines the individual metrics.

Federal department and agency performance towards the Administration's Priority Cybersecurity Capabilities

CAPABILITIES	DOC		DHS		DOD		DOE		DOI		DOJ	
	Q4 FY12	Q1 FY13										
Continuous Monitoring	70	69*	96	90	76	75	74	73	76	84	89	93
PIV Logical Access	10	19	18	18	93	84	0	2	0	19	0	7
TIC Traffic Consolidation	60	85	96	96	N/A	N/A	26	23	98	98	99	99
TIC 2.0 Capabilities (FY13)	74	70	80	80	N/A	N/A	87	88	90	90	94	98

FY13 FISMA Targets

Priority	YELLOW	GREEN
CM	80%	95%
PIV	50%	75%
TIC Traffic	80%	95%
TIC Capabilities	95%	100%

CAPABILITIES	DOL		DOT		EDU		EPA		GSA		HHS	
	Q4 FY12	Q1 FY13										
Continuous Monitoring	90	94	65	60	93	93	39	59	95	95	85	79
PIV Logical Access	0	0	0	0	75	47	0	0	91	93	45	56
TIC Traffic Consolidation	32	83	91	91	80	80	95	95	0	70	0	0
TIC 2.0 Capabilities (FY13)	N/A	N/A	72	72	85	85	N/A	32	N/A	N/A	40	75

N/A indicates that the agency is not responsible to report this TIC score.

- DOD does not report
- MTIPS customers

CAPABILITIES	HUD		NASA		NRC		NSF		OPM		SBA	
	Q4 FY12	Q1 FY13										
Continuous Monitoring	80	83*	90	87	100	100	98	98*	98	99	94	94
PIV Logical Access	0	0	0	1	10	0	0	0	0	26	0	0
TIC Traffic Consolidation	100	100	98	98	100	100	100	100	100	100	100	100
TIC 2.0 Capabilities (FY13)	68	68	85	87	N/A	100	N/A	N/A	92	92	N/A	N/A

FY13 measures TIC 2.0 capabilities

* Indicates FY12 Q4 Configuration Management reporting used for some agencies.

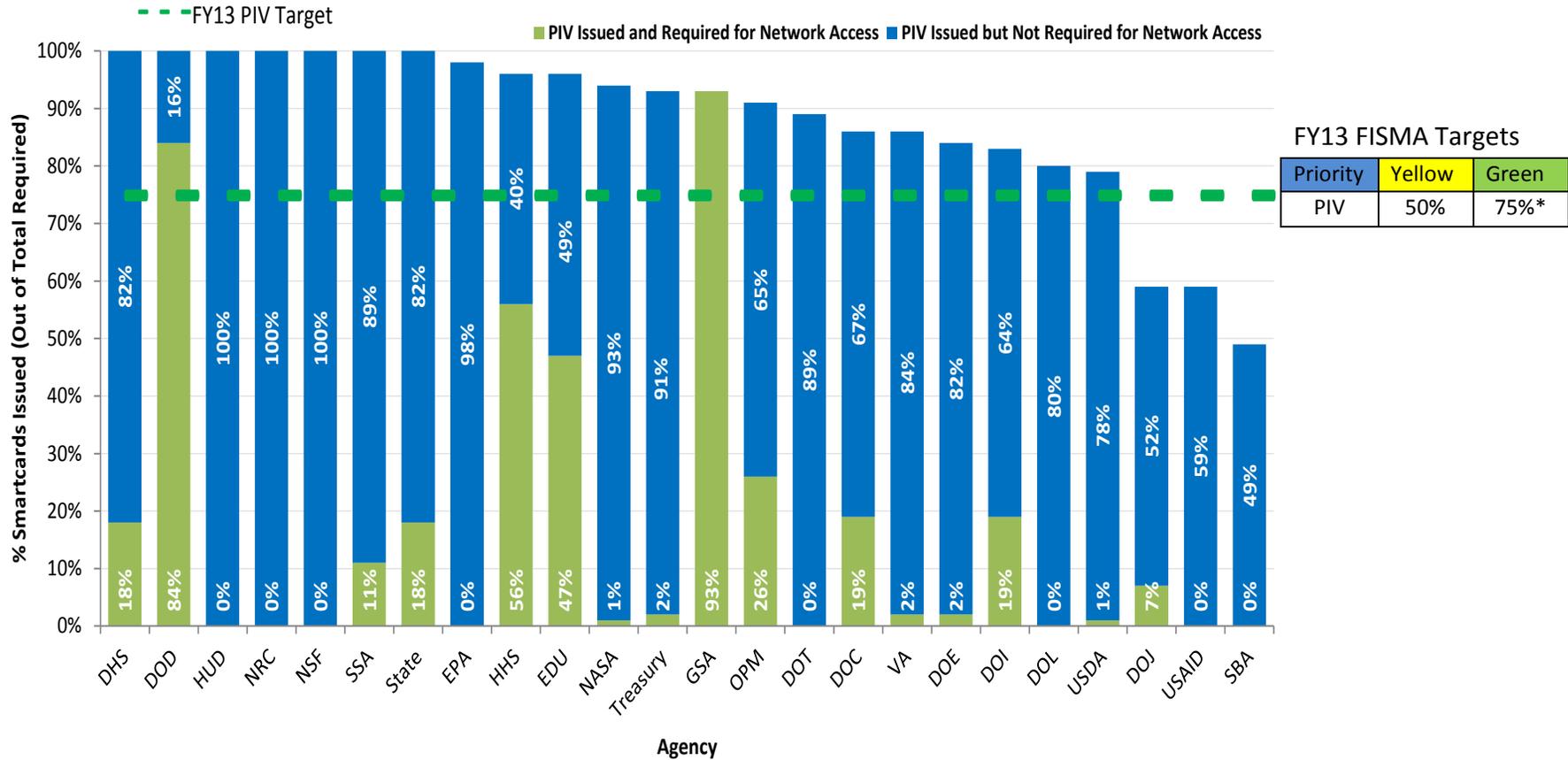
CAPABILITIES	SSA		STATE		TREAS		USAID		USDA		VA	
	Q4 FY12	Q1 FY13										
Continuous Monitoring	82	69	67	67	79	82	100	100	80	79*	67	98
PIV Logical Access	0	11	1	18	0	2	0	0	0	1	2	2
TIC Traffic Consolidation	100	100	100	100	95	95	100	100	100	100	98	19
TIC 2.0 Capabilities (FY13)	91	91	82	86	76	100	N/A	95	73	73	85	80

Federal department and agency performance towards Continuous Monitoring as of Q1 FY2013



* Indicates FY12 Q4 Configuration Management reporting used for some agencies

Federal department and agency performance towards Strong Authentication with HSPD-12 Cards as of Q1 FY2013



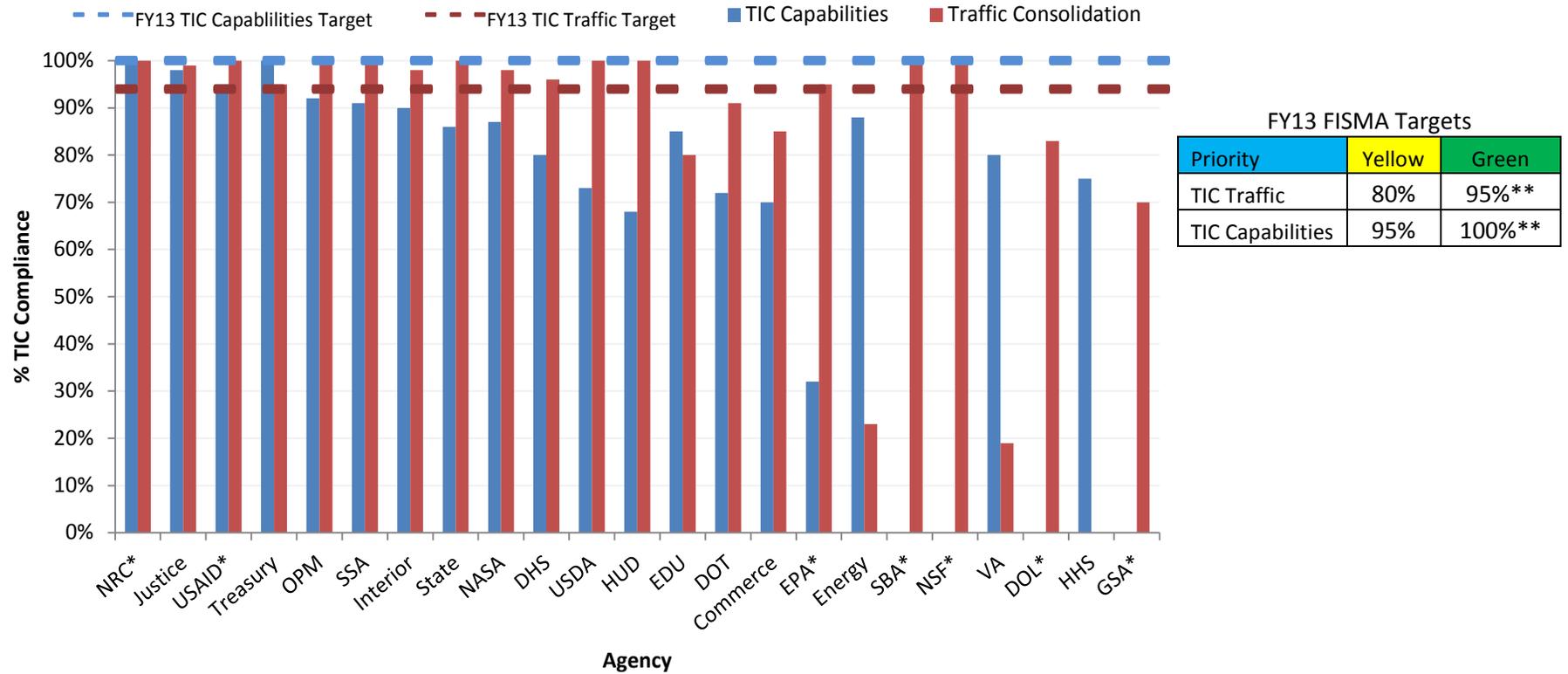
PIV Cards Issued as of September 2012: 5,285,036 (96%)

Percentage of accounts requiring use of PIV cards for network logon: 54%

PIV card issuance data from September 2012. PIV card usage data percentages from January 2013

* Represents FY13 FISMA Targets. PIV targets are set at 75%, and the dotted line on the chart above indicates this target.

Federal department and agency performance towards Trusted Internet Connection (TIC) use and capabilities as of Q1 FY2013



TIC Capabilities represent TIC 2.0 * Agency uses MTIPS provider

TIC Capabilities: Agency FY13 target is 100% ; Government-wide status is 82% (decreased 2% from FY12 Q4 to FY13 Q1)

TIC Traffic Consolidation: Agency FY13 target is 95%; Government-wide status is 84% (increased 3% from FY12 Q4 to FY13 Q1)

**Represents FY13 FISMA Targets. TIC Traffic and TIC Capabilities targets are set at 95% and 100%, respectively, and the dotted lines on the chart indicate these targets.

Key Indicators and Metrics

Agency performance uses the FY2013 FISMA metrics and targets, highlighted in Table 2: FY2013 FISMA Metrics.

Administration Performance Area	Annual FISMA Metric Section ⁶	Performance Metric	Minimal Level	Target Level
Continuous ⁷ Monitoring – Assets	2.2	% of assets in 2.1, where an automated capability (device discovery process) provides visibility at the organization’s enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring – Configurations	3.1.3	% of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and provide visibility at the organization’s enterprise level.		
Continuous Monitoring – Vulnerabilities	4.2	% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization’s enterprise level.		
Strong Authentication -Identity Management HSPD-12	5.2.5, 5.4.5 &10.2.5	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
TIC Consolidation - CNCI ⁸ #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC ⁹).	80%	95%
TIC Capabilities - CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%

Table 2: FY2013 FISMA Metrics

⁶ Section references are to the annual metrics only, and do not apply to the quarterly metrics.

⁷ Continuous does not mean instantaneous. NIST SP 800-137 says that the term “continuous” means that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

⁸ Comprehensive National Cybersecurity Initiative (CNCI)

⁹ Not applicable to Department of Defense (DOD).

Milestones Accomplished to Date (FY13Q1)

Milestone	Status
Q1FY13: NIST: Closed public comments for FIPS 201-2. Adjudicated comments and updated Draft FIPS 201-2 for submission.	Completed
October 2012: Complete Strong Logical Access Tiger Team (SLATT) actions - GSA, Department of Defense (DOD), and Treasury led a Strong Logical Access Tiger Team (SLATT) to identify roadblocks for strong authentication. The SLATT improves strong authentication outcome metrics across agencies by focusing tiger team efforts on critical barriers to implementation and deliverables that can assist in implementation.	Completed
October 2012: Create Joint Continuous Monitoring Working Group (CMWG) - The ISIMC Continuous Monitoring Working Group (CMWG) and the Committee on National Security Systems (CNSS) CMWG combined to create the "Joint CMWG". The Joint CMWG is the central forum for interagency continuous monitoring program coordination for both national security systems and non-national security systems.	Completed
October 2012: NIST, DHS, DOD introduced SCAP automation specifications to the Internet Engineering Task Force (IETF) to ensure industry adoption and inclusion of continuous monitoring capabilities.	Completed
October 17, 2012: NSS and OMB facilitated an interagency coordination plan for continuous monitoring to get concurrence between DHS, NIST, DOD, and agency CIOs and support alignment between National Security Systems and non-National Security Systems.	Completed
October 19, 2012: DHS worked with GSA on a Federal enterprise-wide continuous diagnostics and mitigation (CDM) solicitation announcement.	Completed
November 1, 2012: DHS to provide continuous diagnostics program details to the Joint CMWG to supplement the CONOPS	Completed
November 15, 2012: Agencies report FISMA Metrics to ensure completion of the congressional report in a timely manner.	Completed
November 27, 2012: The Joint CMWG developed a Concept of Operations (CONOPS) for the execution of continuous monitoring on a government-wide basis.	Completed
November 27, 2012: The Joint CMWG provided recommendations for a continuous monitoring program that aligns across national and non-national security domains.	Completed
November 30, 2012: DHS released FY2013 FISMA metrics	Completed
December 12 2012: GSA/FAS US access MSO: The HSPD-12 MSO awarded a 5-year BPA in December 2012 that reduces the wholesale cost of PIV cards by nearly 30%. The first call under that BPA for 100,000 cards will save the MSO over \$400,000 as compared to the price under the core services contract.	Completed
November, 2012: DHS released Continuous Diagnostics Dashboard Request For Information (RFI)	Completed
December, 2012: DHS released Continuous Monitoring As A service (CMaaS) Blanket Purchase Agreement (BPA)	Completed