

Cross Agency Priority Goal: Cybersecurity

FY2013 Q3 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 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
Executive Summary.....	3
Cybersecurity CAP Strategy.....	4
Embrace Federal Information Security Management Principles	5
Cybersecurity CAP Action Plan.....	6
Use the FISMA Governance Structure	7
Cross-Agency Coordination.....	7
Deputy Secretary Coordination	7
Performance Improvement Officer (PIO)/Chief Financial Officer (CFO) Coordination	8
Chief Information Officer (CIO)/Chief Information Security Officer (CISO) Coordination.....	8
National Security Systems Coordination.....	8
Monitoring and Reviewing Progress.....	8
1. Milestones for the Upcoming Quarter (FY2013 Q4).....	10
2. Contributing Programs and Other Factors.....	11
Progress Update.....	13
Scorecards.....	17
Government-wide Scorecards	17
Key Indicators and Metrics	23
Milestones Accomplished to Date (FY13Q3)	24

Executive Summary

The federal government made no significant progress toward the Administration's Priority Cybersecurity Capabilities over the past quarter, with an overall decrease in the capability adoption of 1.14% and a slight decline of 0.51% in mandatory HSPD-12 compliant PIV card use for strong network authentication.

Moreover, all Federal agencies provided an updated capability implementation plan: according to the submissions, the Federal government will not achieve the Cybersecurity Cross Agency Priority (CAP) goal by the end of FY2014.

The White House is reaching out to agency leadership to highlight our concern with this goal and get it back on track, despite the difficult budget environment.

Background

The need to secure government information is not new, and the Federal government has enacted a number of policies and legislation aimed at safeguarding Federal information systems and data. However, the increasing pace of technology adoption, increasing value of information, and increasing reliance on mobility, accessibility, and information sharing for agencies' mission execution has increased the challenge of effectively safeguarding federal information and systems. In addition, increasingly advanced capabilities aimed at disrupting federal IT operations are more readily available to less sophisticated actors and organizations.

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

State and non-state actors increasingly exploit the Internet to achieve strategic objectives. The growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation.¹

Cyber threats to Government information and communications infrastructure, whether from domestic or international criminal elements or nation-states, continue to grow in

¹ *Worldwide Threat Assessment of the US Intelligence Community* : Hearing before the Senate Select Committee on Intelligence, 113th Cong. (2013) (The Honorable James R. Clapper). Retrieved from <http://www.intelligence.senate.gov/130312/clapper.pdf>

number and sophistication, creating the potential that essential services could be degraded or interrupted, and confidential information stolen or compromised, with serious effects.

The federal government recognized this challenge and responded by focusing on priority cybersecurity capabilities with effective defensive successes, and elevating recognition of the cybersecurity threat to senior leadership. Consequences and mission impact of cyber incidents are now part of the risk management calculus, from White House senior leadership to executive cabinet agency leadership. Securing Federal Networks is one of five key cybersecurity priorities highlighted as an important and strategic investment in the FY2014 budget proposal:

Protect Federal IT Assets and Data Through Improved Cybersecurity – 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 Federal government is not just a technology issue. It is also an organizational, people, and performance issue requiring creative solutions to address emerging and increasingly sophisticated threats, and new vulnerabilities introduced by rapidly changing technology. To overcome this challenge, Federal agencies must improve cybersecurity capabilities to provide safe, secure, and effective mission execution and services, with a focus on accountability. Specifically, agencies must continue to implement initiatives such as the Cybersecurity Cross-Agency Priority (CAP) Goal, which is part of the Administration's broader performance management improvement initiative (encompassing Trusted Internet Connections, continuous monitoring and strong authentication), the Federal Information Security Management Act (FISMA), and continuously measure agency progress in improving information security performance through CyberStat reviews.²

Cybersecurity CAP Strategy

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 the FISMA requirement to hold the agency head accountable for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use,

² Analytical Perspectives, FY2014 Proposed Budget of the United States, pp. 349

disclosure, disruption, modification, or destruction of information and information systems. The agency head delegates the authority to ensure information security compliance to the Chief Information Officer (CIO).³

Under the GPRA Modernization Act of 2010, the Chief Operating Officer (COO) shall advise and assist the head of the agency to improve performance and achieve agency mission and goals, with support from the Performance Improvement Officer (PIO). As Cybersecurity is a Cross Agency Priority Goal, the PIO and CIO work together to support the COO to improve agency cybersecurity performance through implementation of the Administration's priority cybersecurity capabilities.

A CIO must be empowered with executive leadership support, authority and resources to direct agency activity to successfully implement these priorities and make progress. The role of the PIO is to assist the CIO with coordinating efforts across the agency while making sure the appropriate performance framework is in place to drive success. Coordination efforts include goal setting and quarterly performance reviews, cross-agency collaboration and coordination, and helping the agency adopt effective practices to improve cybersecurity performance.

Specific to the Cybersecurity CAP goal, under OMB A-11 part 6, the PIO and the CIO work together to improve cybersecurity efforts by:

- (1) Supporting the agency head and COO in leading agency efforts to set cybersecurity goals, make results transparent, review progress and make course corrections
- (2) Reaching out to other component offices to support the CIO to improve cybersecurity effectiveness and efficiency
- (3) Helping components, program office leaders and goal leaders to identify and promote adoption of effective practices to improve cybersecurity outcomes, responsiveness and efficiency.⁴

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

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

³ FISMA of 2002, Section 3544. Federal agency responsibilities

⁴ OMB Circular No. A-11 (2012). Section 200.12 What is the role of the Performance Improvement Officer?

reporting process. Agencies and components are accountable to leadership and the public through increased visibility and reporting frequency. Regular progress reporting occurs through manual and automated data feeds provided 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 significant activities occurring outside the reportable FISMA survey. 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, reliability 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** – Measuring the effectiveness of cybersecurity is challenging, 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.

Cybersecurity CAP Action Plan

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. Federal agencies coordinate with their PIO to submit a CAP Action Plan incorporating their strategic planning process to identify their goals and progress towards achieving the Administration's priority cybersecurity capabilities. 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.

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.

Cross-Agency Coordination

Implementation is 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 Federal CIO Council. The Administration’s priority cybersecurity capabilities use established bodies for cross-agency coordination:

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 OMB⁵ and the same FISMA metrics and operational guidance provided by DHS.

Progress reporting should be no less than quarterly as required under GPRA Modernization.⁶ 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 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.

⁵ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf>

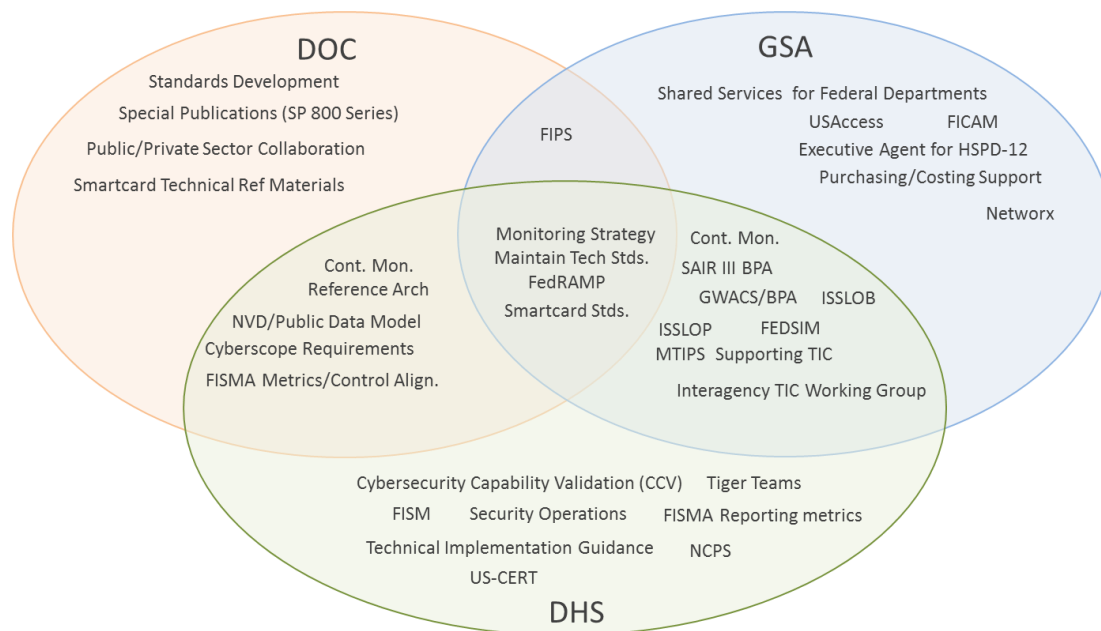
⁶ As stated in the GPRA Modernization Act of 2010 Sec. 1121. *Quarterly priority progress reviews and use of performance information*, the cybersecurity CAP Goal progress will be reviewed to assess whether agencies are making progress towards milestones as planned.

1. Milestones for the Upcoming Quarter (FY2013 Q4)

Milestone	Status
Carry-over from prior quarter (FY2013 Q2)	
The GSA and DHS-chartered tiger team focusing on implementing OMB M-11-11 for strong authentication will evaluate the need for new procurement policy and/or guidance and, if needed, provide policy recommendations to GSA and OMB.	Delayed for policy collection
DHS, Federal Network Resilience (FNR), in collaboration with NCCIC/USCERT will develop a technical analysis that 1). Details the issues and limitations of the current incident reporting methodology, 2). Details the current challenges of correlating FISMA data to security events and outcomes, and 3). Suggests a path forward for the bi-directional alignment of FISMA risk posture data (including SCAP and Sensor feed data) collected by FNR and incident data used by NCCIC/USCERT to provide D/As with improved threat forecasting, risk analysis, and assessment.	Under Development
New Milestones for FY2013 Q4	
NIST to develop recommendations and brief all D/As on mobile device authentication for HSPD-12 compliant two-factor authentication.	
OMB to issue CDM memo and CONOPS	

2. Contributing Programs and Other Factors

The mission areas of the three contributing agencies (Department of Homeland Security, Department of Commerce, and General Services Administration) provide support activities that enable other Federal departments and agencies to implement the Administration's priority cybersecurity capabilities. These include the DHS Federal Network Resilience (FNR), the DOC's National Institute of Standards and Technology (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 report⁷, and continued with the FY2012 and FY2013 FISMA metrics⁸.

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 FY2013 Agency Performance Plans. 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/	
	FY2012Q4	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q4	FY2014Q1	FY2014Q2	FY2014Q3	FY2014Q4	Min	Ta
Continuous Monitoring	79.53%	78.42%	83.58%	82.07%	78.68%	81.27%	82.05%	85.24%	87.12%	91.77%	93.06%	94.90%	80.00%	95.
Strong Authentication	57.26%	53.72%	67.21%	66.70%	61.07%	65.71%	67.42%	72.00%	74.61%	76.89%	78.76%	81.45%	50.00%	75.
TIC Consolidation	81.22%	84.00%	84.39%	84.17%	84.00%	86.48%	89.13%	91.61%	93.09%	93.39%	94.87%	95.35%	80.00%	95.
TIC Capabilities	83.87%	82.21%	85.35%	83.78%	80.96%	84.96%	90.26%	92.13%	92.74%	95.52%	96.70%	98.09%	95.00%	100.
Cyber CAP	76.82%	75.87%	81.28%	80.14%	77.01%	80.16%	82.16%	85.24%	86.97%	90.19%	91.58%	93.27%		

Table 1: Cybersecurity CAP Quarterly targets

⁷ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_e-gov_act_report.pdf

⁸ <http://www.dhs.gov/xlibrary/assets/nppd/ciofismametricsfinal.pdf>

Progress Update

Based on the Q3 FY2013 CyberScope reports on the Administration's priority cybersecurity capabilities, agencies stalled in their progress toward the Cybersecurity Cross Agency Priority (CAP) goals. Agencies continued to focus their attention on the CAP priority capabilities, but while last quarter saw significant improvement, further advancement this quarter proved to be more difficult. The chart below represents the results of the quarterly FISMA reporting for FY2013 Q2 and Q3 for the Administration's priority cybersecurity capabilities.

	USG-Wide Quarterly Results		USG-Wide CAP Target	
	FY2013 Q2	FY2013 Q3	Target FY2013	Target FY2014
Continuous Monitoring	83.58%	82.07%	87%	95%
Strong Authentication	67.21%	66.70%	74%	90%
TIC Consolidation	84.39%	84.17%	88%	95%
TIC Capabilities	85.35%	83.78%	92%	100%
Weighted Average	81.28%	80.14%	85.83%	95%

FISMA Metrics

The FY2013 Q2 FISMA reporting showed considerable progress across the board on the Administration's CAP priority cybersecurity capabilities. Some of this progress may be attributable to relatively easily achievable gains that required modest effort. Agencies may have chosen a course of action that produced quick and easily obtainable results as part of the march towards the CAP goals. It was expected that this rate of improvement would be difficult to sustain and that proved to be the case for FY13 Q3. Although no capability area improved, no capability backslid more than two percentage points.

For Continuous Monitoring there were almost a million more assets reported by the CFO agencies. Only half these additional assets were under automated asset inventory or vulnerability management and this dropped the overall score for each by 5%. While a third of the additional assets were attributable to the normal fluctuation in DOD reporting, most of the remainder were due to an increase in the scope of reporting and the installation of new tools. This is a natural outcome of improving continuous monitoring capabilities: as agencies focus on the deployment of continuous monitoring tools they will initially identify more assets. Accordingly, scores will fluctuate and occasionally decline before showing steady improvement.

One of the items discussed at the CyberStat review for the Department of Energy (DOE) was the desire to have the laboratories (M&O) participate in DOE FISMA reporting. That participation began this quarter, leading to dramatic increases in the DOE total number of assets. Since this reporting was new to those involved, there is anticipation that the

percentage reported under management will increase as they track these ongoing. Another big increase in reported assets came from VA as they installed a new asset discovery tool to augment their existing toolset. This led to a 250,000 increase in the number of assets reported but no increase in the number of assets under automated asset or vulnerability management. It is expected that the ability to see and report on those additional assets will be followed shortly with vulnerability management and secure configuration management capabilities.

The increased scope and the increased implementation of discovery tools should lead to better future scores and the coverage of the federal government will be more complete and comprehensive. Although this quarter experienced a temporary setback in overall CAP Continuous Monitoring percentage, one should not lose sight of the fact that in absolute numbers there were several highlights for Q3 including (non-DOD):

- 295,000 additional assets under configuration management
- 418,000 additional assets under asset inventory management
- 363,000 additional assets under vulnerability management

There was a slight dip of 0.51% in the Strong Authentication PIV score even as many agencies improved their posture. Most of the change was due to DOD remote access PIV users declining by more than 90,000. PIV use in GSA, SSA, and DOI increased more than 10% in Q3. Absent DOD, the PIV score for the other CFO agencies rose 2.62% as:

- 75,000 additional workplace users were required to logon with PIV
- 35,000 additional remote access users were required to logon with PIV

The TIC 2.0 Capabilities metric decreased by 1.5% as more agencies relied on the Cybersecurity Compliance Validation (CCV) assessment score for reporting purposes. The CCV assessments, which include site visits, are a more accurate measure of the TIC security capability requirements in place. Since the TIC metrics are an average of the agency percentages, a significant drop by a single agency can have considerable effect on the overall number. This occurred in Q3 as DOC used the CCV value, which was 33% lower than their reported score for Q2. This alone caused the overall TIC 2.0 Capabilities score to drop 1.44%. For TIC Consolidation fifteen of the twenty-three agencies (DOD is exempt) have achieved the CAP goal of 95%, and another four have reached the minimum target.

Last quarter DOD, through its asset and personnel size, heavily influenced the government wide numbers used to compute the CAP scores. Although DOD could still drive the government averages in either direction, for this quarter, DOD numbers did not disproportionately influence the direction or total of the CAP score. The CAP score fell 1.14% from Q2 to Q3 but without DOD, it would have fallen 1.02%.

FY2013 Q3 Summary

- The overall Cyber CAP score decreased by 1.14% from FY13 Q2 to FY13 Q3 as the implementation of each priority cybersecurity capability realized no gains.
 - The overall Continuous Monitoring score decreased 1.51% as agencies reported more assets but those assets have not yet been determined to be under management.
 - TIC 2.0 Capabilities decreased 1.57% and TIC Consolidation decreased 0.22% as agencies continued to migrate to the TIC 2.0 architecture.
 - Strong Authentication decreased 0.51% as the number of remote access users required to use PIV continued to fluctuate.
- Continuous Monitoring
 - Government-wide, the Automated Asset Management score fell 5.75% and now stands at 84.78% as DOD and VA reported an additional 500,000 assets that were not under asset management. Twenty agencies have reached the minimum target of 80% for Automated Asset Management and sixteen have reached or exceeded the goal of 95%.
 - Automated Vulnerability Management decreased 4.63% as additional unmanaged assets were reported.
 - Automated Configuration Management rose 5.84% as agencies reported on assets with baselines defined by the NIST National Vulnerability Database.
 - Agencies deemed on average that 71% of assets were applicable to Configuration Management while seven agencies reported on all assets for Configuration Management.
- Strong Authentication
 - In FY13 Q3 an additional 7% unprivileged and 2.5% remote access users were reported than in FY13 Q2. While PIV use for the unprivileged users increased 7.5%, for remote access users it decreased 4.5%.
 - Without DOD, the USG PIV implementation score for the other 23 CFO agencies would have risen 2.62%.
 - One-third (8) of the agencies are still at 0% for PIV implementation and another one-quarter (6) are at 6% or less.
 - DOD, GSA and EDU are the only agencies reporting at or above the FY2013 goal of 75%.
 - HHS is reporting above the FY13 FISMA minimum of 50% and SSA and DOI continue to make significant progress towards that target.
- Trusted Internet Connection (TIC)
 - Nineteen of the 23 CFO agencies (DOD is exempt from this reporting) achieved the minimum FY 13 FISMA target of 80% consolidation with 15 reaching the CAP goal of 95%.

- DOE, HHS, VA and DOC remain below the TIC Consolidation minimum.
- VA reported their annual CCV assessment value and it will not change until Q2 FY14.

Progress with Continuous Monitoring is expected to accelerate with the recent announcement of the Continuous-Monitoring-as-a-Service (CMaaS) Blanket Purchase Agreement (BPA) to support the Continuous Diagnostics and Mitigation Program (CDM).

Through the CDM program⁹, DHS works with partners across the entire Federal executive branch civilian government to deploy and maintain an array of sensors for hardware asset management, software asset management and whitelisting, vulnerability management, compliance setting management and feed data about an agency's cybersecurity flaws and present those risks in an automated and continuously updated dashboard. CDM, which will also be available for state and local entities as well as the defense industrial base sector, provides stakeholders with the tools needed to protect their networks and enhance their ability to see and counteract day-to-day cyber threats.

⁹ Additional information regarding the CDM and CMaaS BPA can be found at: <http://www.gsa.gov/cdm>

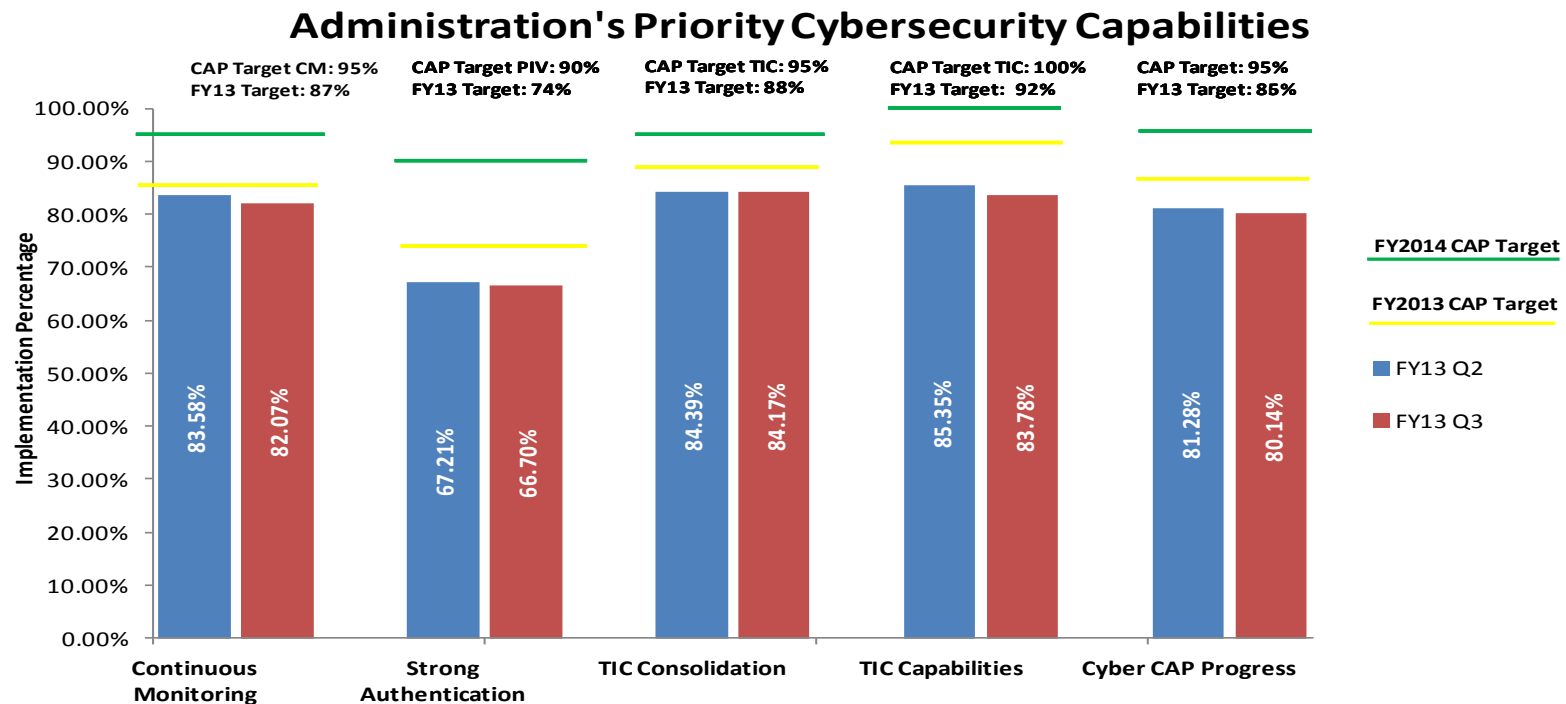
Scorecards

The series of graphs below represent two types of scorecards. The first set shows government-wide performance towards the Administration's Priority Cybersecurity Capabilities. The FY2013 FISMA metrics provide 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 Scorecards

The next two charts show the progress towards the CAP priority cybersecurity capability goals across the government for the 24 Chief Financial Officer (CFO) agencies. The first chart shows the quarterly progress from Q2 FY13 to Q3 FY13.

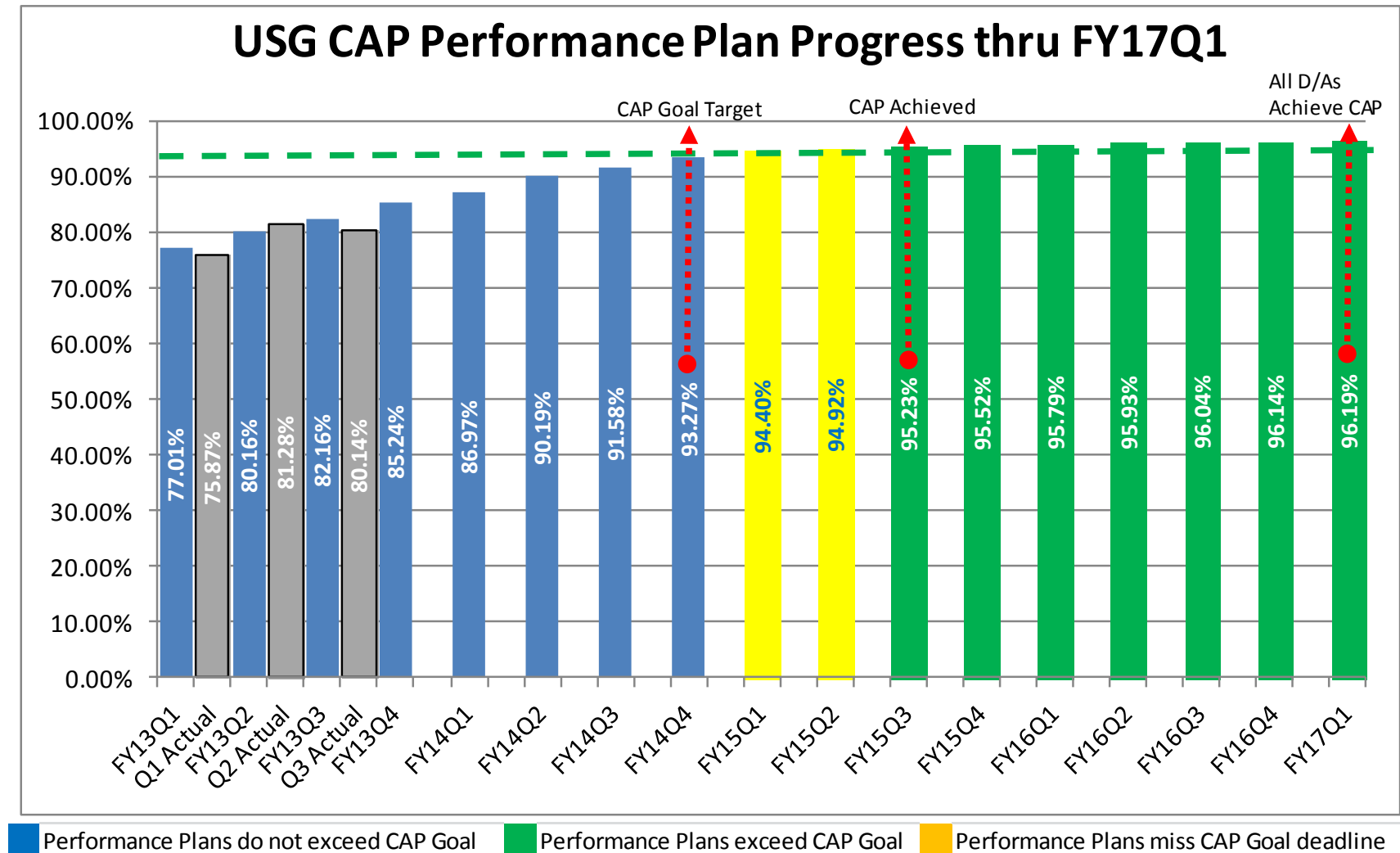
Government-wide performance towards the Administration's Priority Cybersecurity Capabilities as of FY13 Q3



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

The chart below shows the actual FY13 progress and the USG planned progress through the end of FY16. As depicted by the chart, the USG is not on target to reach the CAP goals by Q4FY14 based on the agency performance plans.

Government-wide performance towards the Administration's Priority Cybersecurity Capabilities



Federal department and agency performance for FY2013 Q2 – Q3 relative to Agency Performance Plans


The table below shows each agency's contribution to the achievement of the individual cybersecurity capabilities. Increasing shades of green indicates agencies ahead of their planned performance plan, while increasing shades of red indicate agencies below their planned performance plan. Yellow indicates zero (0) for both planned and actual performance improvement.


CAPABILITIES	DOC				DHS				DOD				DOE				DOI				DOJ			
	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan
Continuous Monitoring	63	69	61	69	87	80	90	85	79	78	79	78	90	73	85	78	87	76	92	81	94	90	99	92
PIV Logical Access	18	20	23	22	21	29	23	33	92	90	92	90	4	0	6	27	30	15	41	18	13	15	17	26
TIC 2.0 Capabilities	74	80	41	80	87	85	91	90	N/A	N/A	N/A	N/A	88	85	88	90	77	92	85	98	98	98	88	98
TIC Traffic Consolidation	71	85	70	86	72	85	82	90	N/A	N/A	N/A	N/A	22	40	19	50	99	98	99	99	99	99	81	99

CAPABILITIES	DOL				DOT				EDU				EPA				GSA				HHS			
	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan
Continuous Monitoring	91	92	94	99	52	73	48	51	95	93	98	93	64	45	63	45	93	93	95	93	87	89	87	90
PIV Logical Access	0	0	0	0	0	1	0	0	75	87	75	87	0	0	0	0	48	48	96	48	63	61	62	65
TIC 2.0 Capabilities	100	100	100	100	72	100	62	62	85	85	85	85	32	80	32	82	100	0	100	100	80	80	80	100
TIC Traffic Consolidation	100	100	100	100	91	95	99	95	80	80	91	80	95	95	95	95	100	100	100	100	0	0	0	40

CAPABILITIES	HUD				NASA				NRC				NSF				OPM				SBA			
	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan
Continuous Monitoring	86	79	89	85	96	90	96	91	100	96	97	96	93	100	95	100	99	100	99	100	99	33	70	33
PIV Logical Access	0	0	0	0	1	1	1	5	0	0	0	0	0	0	0	0	4	8	4	44	0	0	0	25
TIC 2.0 Capabilities	68	69	68	69	87	88	88	88	100	100	100	100	100	100	100	100	92	92	92	100	100	100	100	100
TIC Traffic Consolidation	100	100	100	100	98	99	98	99	100	100	100	100	100	100	100	100	100	100	100	100	100	99	84	99

CAPABILITIES	SSA				STATE				TREAS				USAID				USDA				VA			
	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan	Q2 FY13	Perf Plan	Q3 FY13	Perf Plan
Continuous Monitoring	82	86	96	94	76	84	84	84	80	80	78	77	99	98	100	98	100	100	100	100	100	95	77	95
PIV Logical Access	11	11	30	12	1	1	4	4	3	3	3	31	0	0	0	0	20	2	20	25	2	7	5	0
TIC 2.0 Capabilities	91	91	96	95	80	80	82	80	95	92	92	92	95	95	95	100	80	80	80	85	82	82	82	82
TIC Traffic Consolidation	100	100	100	100	100	100	100	100	95	95	99	99	100	100	100	100	100	100	100	100	19	19	19	19

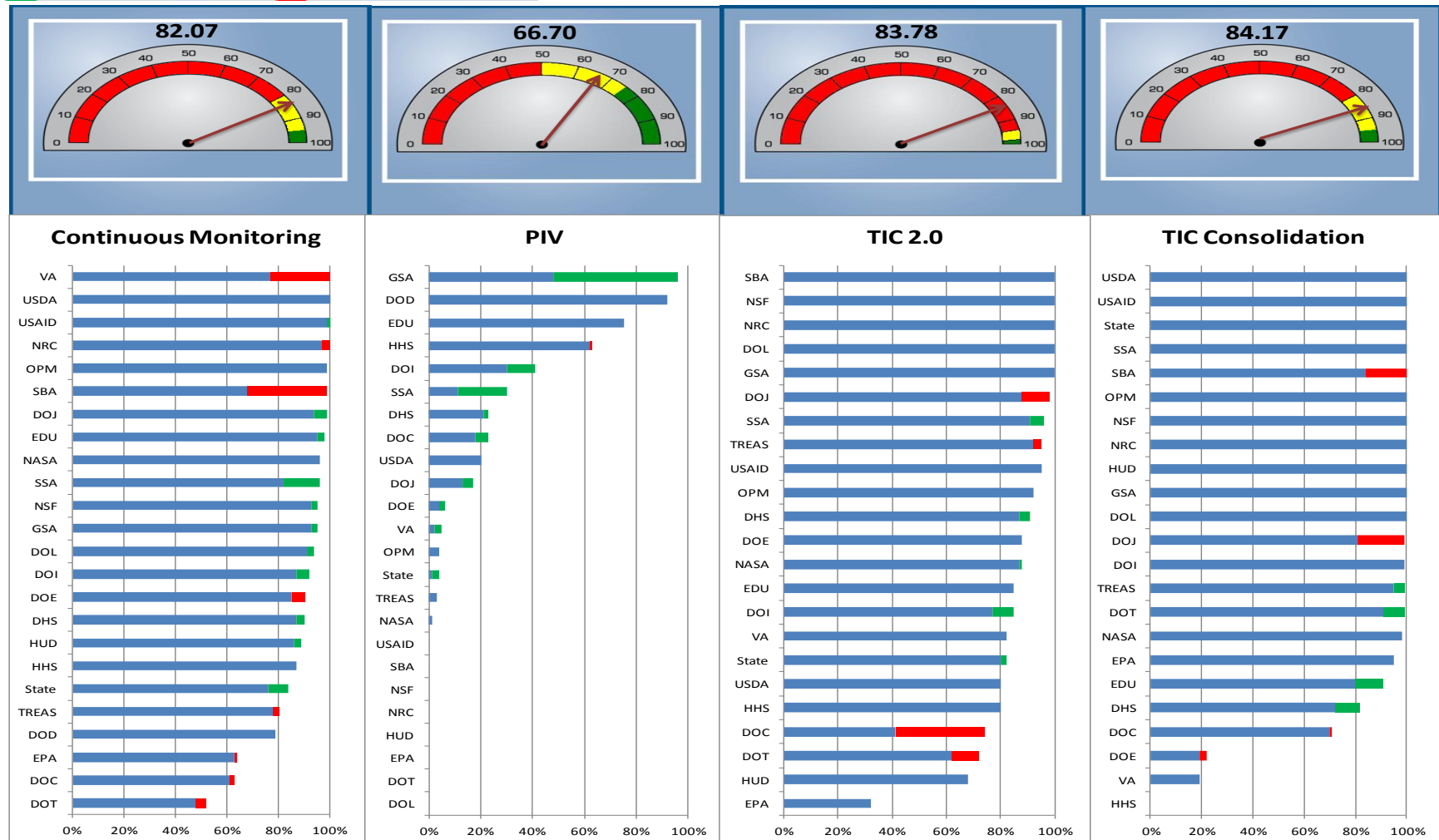
 Q3 < Performance Plan
 → Worse

 Q3 => Performance Plan/Goal
 → Better

Federal department and agency performance for FY2013 Q2 – Q3

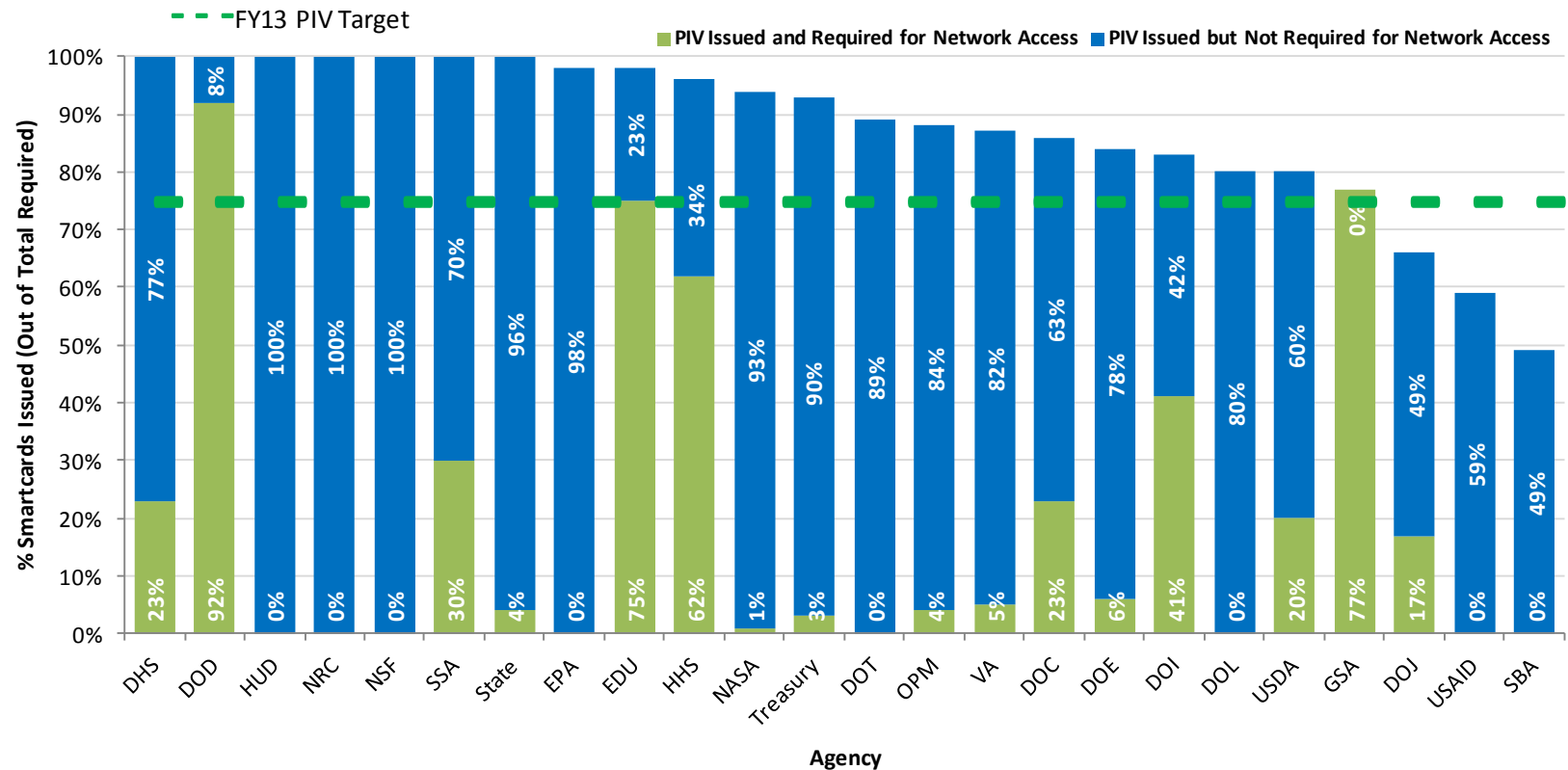
The chart below shows each agency's increase (green) or decrease (red) from FY2013 Q2 to Q3. In most cases, a decrease was a result of more accurate reporting and not a decrease in capabilities. Most decreases were due to a stricter interpretation of the reporting metric, or identification of previously unidentified assets.

■ Q2 Increase from Q1
 ■ Q2 decrease from Q1



Federal department and agency performance towards Strong Authentication with HSPD-12 Cards as of Q3 FY2013

The chart below shows the percentage of agency employees with HSPD-12 cards, and the percentage required to use their cards to authenticate for network access.



PIV Cards Issued as of March 31, 2013: 5,315,299 (96%)

Percentage of accounts requiring use of PIV cards for network login: 67%

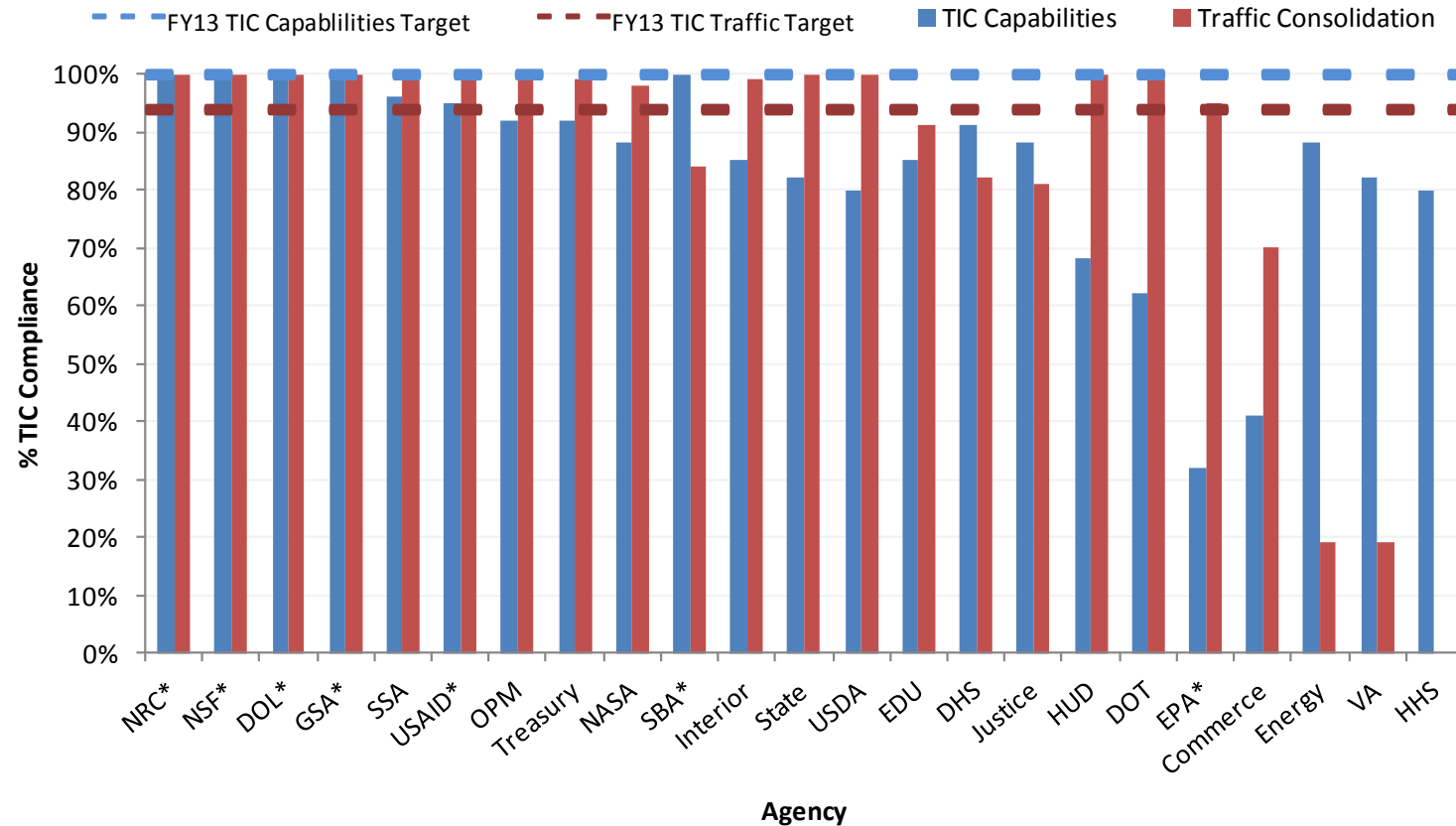
PIV card issuance data from March 2013. PIV card usage data percentages from July 2013

PIV targets are set at 75%, and the dotted line on the chart above indicates this target.

GSA reported 96% usage and 77% issuance.

Federal department and agency performance towards Trusted Internet Connection (TIC) use and capabilities

The chart below shows the percentage of TIC traffic and TIC 2.0 capabilities at each agency as of Q3 FY2013.



TIC Capabilities represent TIC 2.0 * Agency uses MTIPS provider

TIC Capabilities: Agency FY13 target is 100% ; Government-wide status is 84% (decreased 1% from FY13 Q2 to FY13 Q3)

TIC Traffic Consolidation: Agency FY13 target is 95%; Government-wide status is 84% (the same as in FY13 Q2)

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 ¹⁰	Performance Metric	Minimal Level	Target Level
Continuous ¹¹ 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 ¹² #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC ¹³).	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

¹⁰ Section references are to the annual metrics only, and do not apply to the quarterly metrics.

¹¹ 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.

¹² Comprehensive National Cybersecurity Initiative (CNCI)

¹³ Not applicable to Department of Defense (DOD).

Milestones Accomplished to Date (FY13Q3)

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.	Completed
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:	Underway
<ul style="list-style-type: none"> • Develop a PIV Logical Access Control System (LACS) business case 	Completed
<ul style="list-style-type: none"> • Develop a methodology and conduct PIV LACS-related cost and savings analysis 	Completed
<ul style="list-style-type: none"> • Develop standard language for use by requiring officials in acquisitions to support PIV enablement and PIV compatibility and interoperability 	Completed
<ul style="list-style-type: none"> • Identify existing procurement vehicles and investigating new vehicles to provide PIV LACS Technical Support with input from the SLATT needs assessment. 	Complete - templates to be delivered
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.	Coordination started and timeline delivered
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.	Completed
March 31, 2013: DHS, in coordination with the Joint Continuous Monitoring Working Group (JCMWG), define program implementation responsibilities.	Completed
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.	Completed for near-term
March 31, 2013: DHS will collect performance plans and measure performance to see if D/As will hit their targets.	Completed