Cross Agency Priority Goal: Cybersecurity
FY2013 Q2 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

Executive Summary

The federal government has made significant progress toward the Administration's Priority Cybersecurity Capabilities over the past quarter, with an overall increase in the capability adoption of 5.41% and significant improvement of 13.49% in mandatory HSPD-12 compliant PIV card use for strong network authentication.

However, there is significant work remaining. All Federal agencies provided an updated capability implementation plan, and the Federal government will not achieve the Cybersecurity Cross-Agency Priority (CAP) goal by the end of FY2014 based on current performance plans.

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 effective mission execution of federal departments and agencies 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 nonstate 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 number and sophistication, creating the potential that essential services could be degraded or interrupted, and confidential information stolen or compromised, with serious effects.

[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

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 Goal 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, disclosure, disruption, modification, or destruction of information and information

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

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.

Specifically 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 reporting process. Agencies and components are accountable to leadership and the

[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?

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 Goal 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 OMB[5] 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. Longer-term Milestones

Long-term milestones address strategic capabilities and achievements beyond the scope of a single quarter. These include common capabilities and achievements of government-wide capabilities and applicable to all departments and agencies. As a result, these are reported on an annual basis, and listed here for reference.

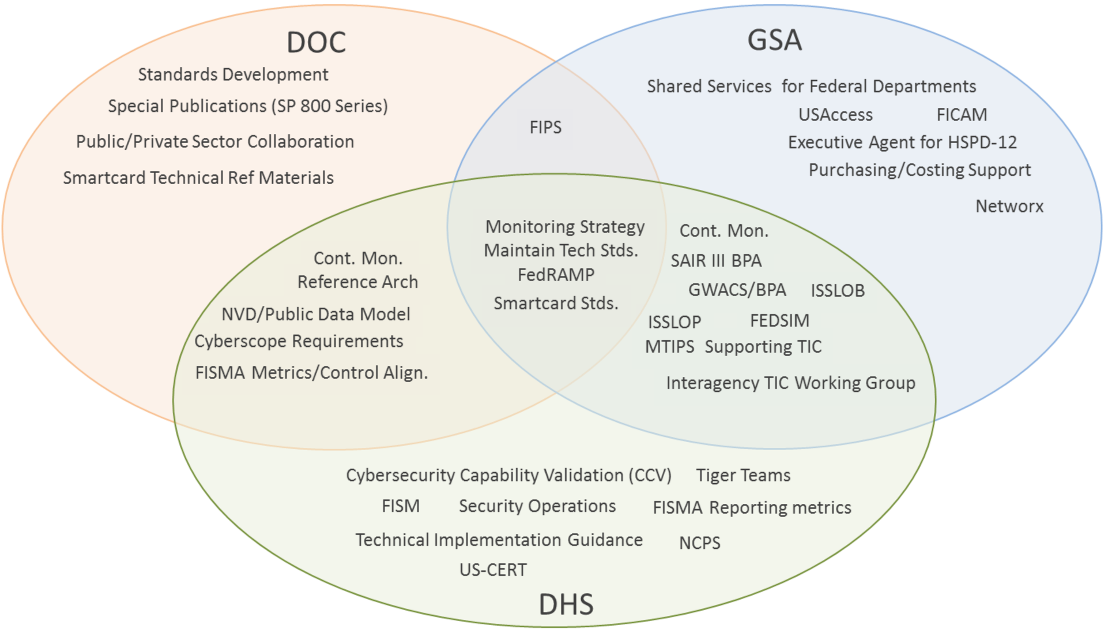
Milestone
All Deputy Secretaries meet at least annually with PIOs and CIOs to review Cybersecurity CAP goal progress.
All PIOs and CIOs meet at least quarterly to review Cybersecurity CAP goal progress.
All departments and agencies report continuous diagnostics data to DHS and DHS integrates to reporting 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 Q3)

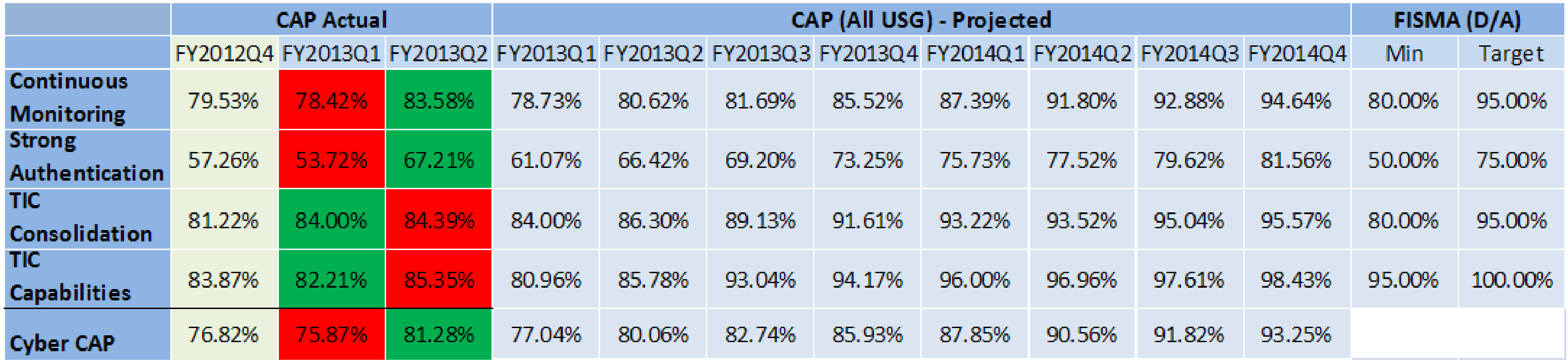
Milestone	**Status**
Carry-over from prior quarter (FY2013 Q2)	
GSA and DHS, working through the CXO Councils, will charter one or more tiger teams focusing on the implementation of OMB M-11-11 for strong authentication to networks and information systems, comprised of participants from CFO Act agencies, to:	Underway
• Collect and evaluate D/A policies and implementing processes related to PIV LACS and develop policy recommendations	Underway
• Identify USG-enterprise systems and/or websites for priority consideration/decision to PIV-enable and mandate PIV usage.	Initiated and ongoing
• Evaluate the need for new procurement policy and/or guidance and, if needed, provide policy recommendations to GSA and OMB	Delayed for policy collection
GSA and NIST to develop a "solutions to PIV implementation barriers" document for D/As to accelerate prioritization and implementation of PIV mandatory authentication.	Delayed: Under Development
DHS to perform at least three CyberStats, focusing specifically on PIV LACS mandatory authentication performance	Two of three CyberStats completed
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.	Under Development
DHS, in coordination with the JCMWG, develop mid-term CDM deployment roadmap specifying deployment milestones, activities to accomplish the plan, and targeted CDM capabilities.	Under Development
DHS, in coordination with the JCMWG, develop a long term CDM operational framework with enough detail to serve as a rough basis-of-estimate for out-year budget projections and guidance.	Under Development
New Milestones for FY2013 Q3	
GSA to collect list of all PIV mobile enrollment workstations in use by Federal D/As lead effort to optimize mobile enrollment workstation use and deployment.	
NIST to develop recommendations and brief all D/As on mobile device authentication for HSPD-12 compliant two-factor authentication.	

3. 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).


DOC
Standards Development
Special Publications (SP 800 Series)
Public/Private Sector Collaboration
Smartcard Technical Ref Materials
GSA
Shared Services for Federal Departments
USAccess
FICAM
Executive Agent for HSPD-12
Purchasing/Costing Support
Networx
FIPS
Monitoring Strategy
Maintain Tech Stds.
FedRAMP
Smartcard Stds.
Cont. Mon.
Reference Arch
NVD/Public Data Model
Cyberscope Requirements
FISMA Metrics/Control Align.
Cont. Mon.
SAIR III BPA
GWACS/BPA
ISSLOB
ISSLOP
FEDSIM
MTIPS Supporting TIC
Interagency TIC Working Group
Cybersecurity Capability Validation (CCV)
Tiger Teams
FISM
Security Operations
FISMA Reporting metrics
Technical Implementation Guidance
NCPS
US-CERT
DHS

The FY2011 FISMA program introduced the Administration's priority cybersecurity capabilities and reported progress through the FY2011 FISMA report[7], and continued with the FY2012 and FY2013 FISMA metrics[8].
FISMA minimum 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.



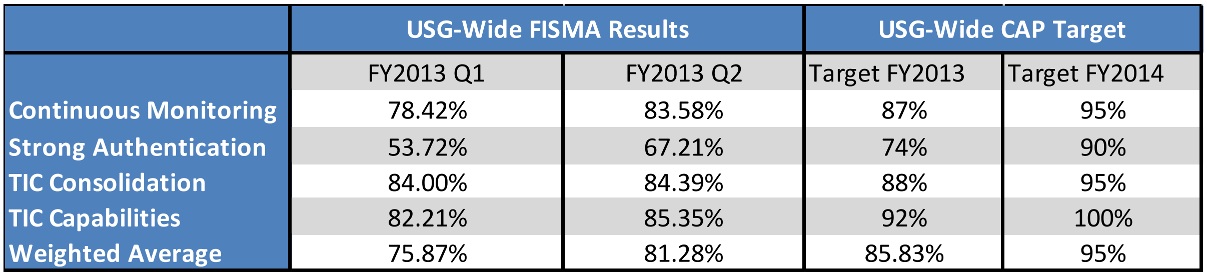
	CAP Actual			CAP (All USG) - Projected								FISMA (D/A)	
	FY2012Q4	FY2013Q1	FY2013Q2	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q4	FY2014Q1	FY2014Q2	FY2014Q3	FY2014Q4	Min	Target
Continuous Monitoring	79.53%	78.42%	83.58%	78.73%	80.62%	81.69%	85.52%	87.39%	91.80%	92.88%	94.64%	80.00%	95.00%
Strong Authentication	57.26%	53.72%	67.21%	61.07%	66.42%	69.20%	73.25%	75.73%	77.52%	79.62%	81.56%	50.00%	75.00%
TIC Consolidation	81.22%	84.00%	84.39%	84.00%	86.30%	89.13%	91.61%	93.22%	93.52%	95.04%	95.57%	80.00%	95.00%
TIC Capabilities	83.87%	82.21%	85.35%	80.96%	85.78%	93.04%	94.17%	96.00%	96.96%	97.61%	98.43%	95.00%	100.00%
Cyber CAP	76.82%	75.87%	81.28%	77.04%	80.06%	82.74%	85.93%	87.85%	90.56%	91.82%	93.25%		

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 Q2 FY2013 CyberScope reports on the Administration's priority cybersecurity capabilities, agencies have made substantial progress toward the Cybersecurity Cross-Agency Priority (CAP) goals. The increase in overall CAP scores reflects continued agency attention and focus to the priority capabilities. The chart below represents the results of the quarterly FISMA reporting for FY2013 Q1 and Q2 for the Administration's priority cybersecurity capabilities.



	USG-Wide FISMA Results		USG-Wide CAP Target	
	FY2013 Q1	FY2013 Q2	Target FY2013	Target FY2014
Continuous Monitoring	78.42%	83.58%	87%	95%
Strong Authentication	53.72%	67.21%	74%	90%
TIC Consolidation	84.00%	84.39%	88%	95%
TIC Capabilities	82.21%	85.35%	92%	100%
Weighted Average	75.87%	81.28%	85.83%	95%

FISMA Metrics

The FY2013 Q2 FISMA reporting shows considerable progress across the board on the Administration's CAP priority cybersecurity capabilities. Each capability area improved with the most significant increase occurring in the category of Strong Authentication using PIV cards for logical network access. However, it is important to note that DoD contributes a significant portion of that improvement.

Of the 24 CFO-Act agencies, the Department of Defense (DOD) contains just over half the assets and reported two-thirds of the users with access to the network. The sheer size of DOD heavily determines the USG progress towards certain Cybersecurity CAP goal targets. DOD implements PIV well and not only reported a significant increase in PIV usage but also a large increase in the number of users remotely and interactively accessing the network. By reporting almost two million more instances of PIV use than in FY13 Q1, DOD single-handedly drove the CAP PIV score up double digits. There is a risk in the fact that DOD personnel numbers can fluctuate dramatically. Those same two million additional accesses may disappear next quarter resulting in a considerable decrease for PIV use. The CAP minimum level or target level may be reached one quarter but not in subsequent quarters. A secondary risk is that in FY2013 Q2, DOD alone causes the USG to reach the FY2014 minimum target for PIV. This may take away the urgency from other agencies to accelerate their progress towards the CAP goal.

The FY2013 FISMA metrics for Strong Authentication include remote access and require the use of PIV cards for remote authentication. An increase in PIV use for remote authentication helped raise the overall score for Strong Authentication. However, this increase may plateau at some time in the future unless agencies can be convinced to change the preferred multifactor authentication from their current embedded methods. Several agencies reported that 100% of their remote access users use some alternate form of two-factor authentication other than PIV cards. They pose the argument that they are already using strong authentication and need to see a cost/benefit analysis to make the change to PIV.

Since not all the assets that agencies reported have a configurable baseline defined, agencies reported on the applicable assets for Automated Configuration Management. While the Automated Configuration Management metric stayed the same, CyberScope presented the agencies with a drop down list of all the defined baselines from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). By reporting on an applicable subset of assets, which excluded assets such as USB thumb drives, there was a considerable increase in the Automated Configuration Management score. This approach not only adds to the ease and detail of reporting, but also allows for deeper analysis of the configuration baselines in use across the government.

The TIC Capabilities metric is now measuring version 2.0, and agencies reported the highest ever compliance, eliminating concern that the migration to TIC 2.0 would cause a prolonged drop in scores. While this progress is welcome, agency performance plans fall short of the FY2014 CAP goal for TIC 2.0 Capabilities. Additionally, only two-thirds of agencies achieve the CAP goal for TIC Consolidation by FY2014, though the USG CAP goal remains on target for 95% consolidation of all USG traffic by FY2014 Q4.

FY2013 Q2 Summary

- The overall Cyber CAP score increased by 5.41% from FY13 Q1 to FY13 Q2 as the implementation of each priority cybersecurity capability realized gains.
    - The overall Continuous Monitoring score increased 5.16% as more detailed configuration management information was captured.
    - TIC 2.0 Capabilities increased 3.14% and TIC Consolidation increased 0.39% as agencies continued to migrate to the TIC 2.0 architecture
    - Strong Authentication increased 13.49% even as agencies reported 2 million more user access paths to the network.
- Continuous Monitoring
    - Twenty agencies have reached the minimum target of 80% for Automated Asset Management and eleven have reached or exceeded the goal of 95%. Government-wide, the Automated Asset Management score rose 2.16% and now stands at 90.53%.
    - Automated Vulnerability Management increased 2.09% as State, SSA, and USDA made improvements of 30% or better.

  - Automated Configuration Management rose 11.24% as agencies reported on assets with baselines defined by the NIST National Vulnerability Database.
  - Agencies deemed on average that 78% of assets were applicable to Configuration Management while ten agencies reported on all assets for Configuration Management.
- Strong Authentication
  - In FY13Q2 an additional 800,000 unprivileged and 20,000 privileged users, as well as 1,140,000 more remote access users were reported than in FY13 Q1. The vast majority of these additional users came from the personnel fluctuations of DOD. Since DOD has historically implemented PIV well, this was the main driver in the surge of the USG PIV score.
  - Without DOD, the USG PIV implementation score for the other 23 CFO agencies would have risen 2.72%, but the CAP Goal of 75% moves back two full years.
  - One-third (8) of the agencies are still at 0% for PIV implementation and another one-quarter (6) are at 5% or less.
  - DOD 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 GSA is approaching that target. DOI and USDA made significant progress and DOJ and HHS made considerable advances as well.
  - Remote access numbers are fluctuating as some agencies are finding their way with the new remote access factor.
  - GSA decreased due to a misunderstanding of account-based remote access.
- Trusted Internet Connection (TIC)
  - Eighteen of the 23 CFO agencies (DOD is exempt from this reporting) achieved the minimum FY 13 FISMA target of 80% consolidation with 16 reaching the CAP goal of 95%. GSA made significant gains to reach the minimum.
  - DOE, HHS, and VA are below the TIC Consolidation minimum and DHS and DOC have slipped back below as well. VA has latency-sensitive issues with medical centers and universities, DOC is using a new assessment methodology for compliance, and DHS had a recent discovery of previously unknown connections.
  - Of the 16 TICAPS, Treasury and DOJ have reached the FY13 FISMA minimum target of 95% for TIC 2.0 Capabilities.
  - The seeking service agencies using an MTIPS vendor (DOL, GSA, EPA, NRC, NSF, SBA and USAID) scored at 100% for TIC Capability unless they reported otherwise.

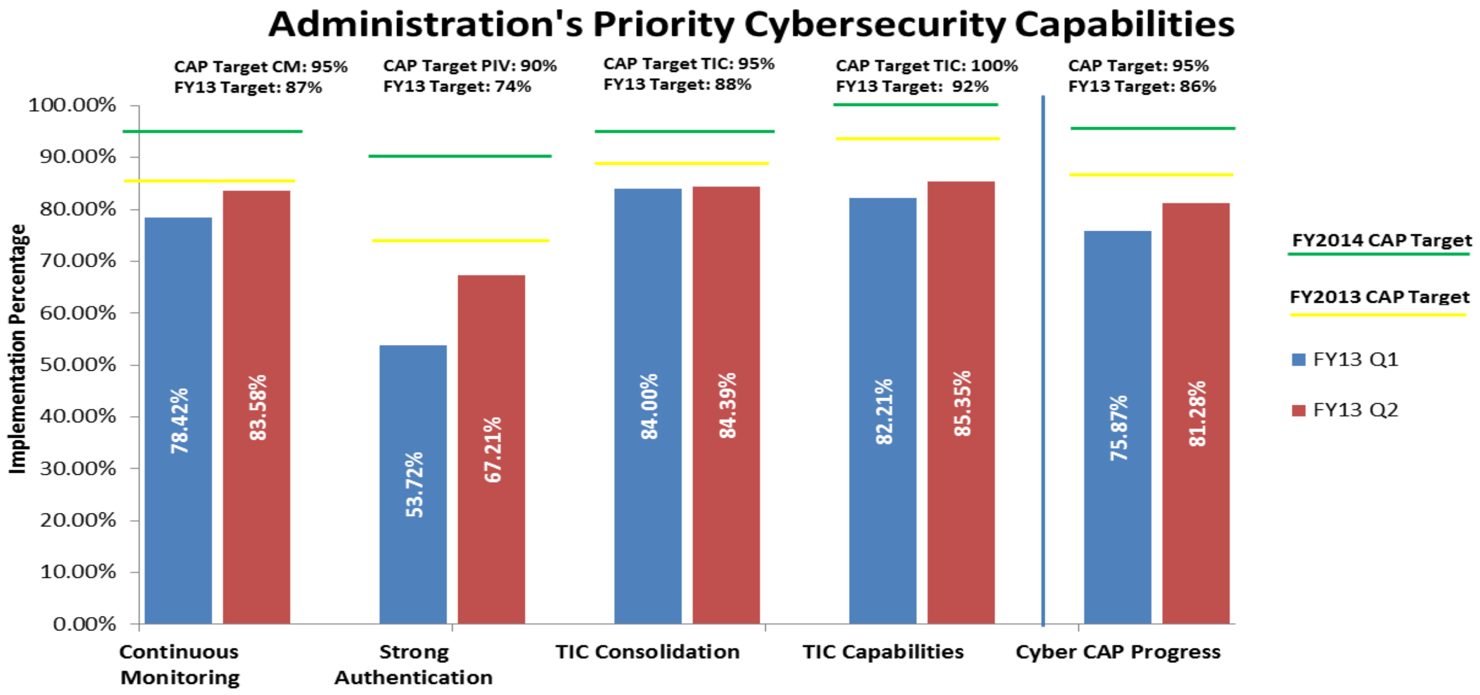
Scorecards

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

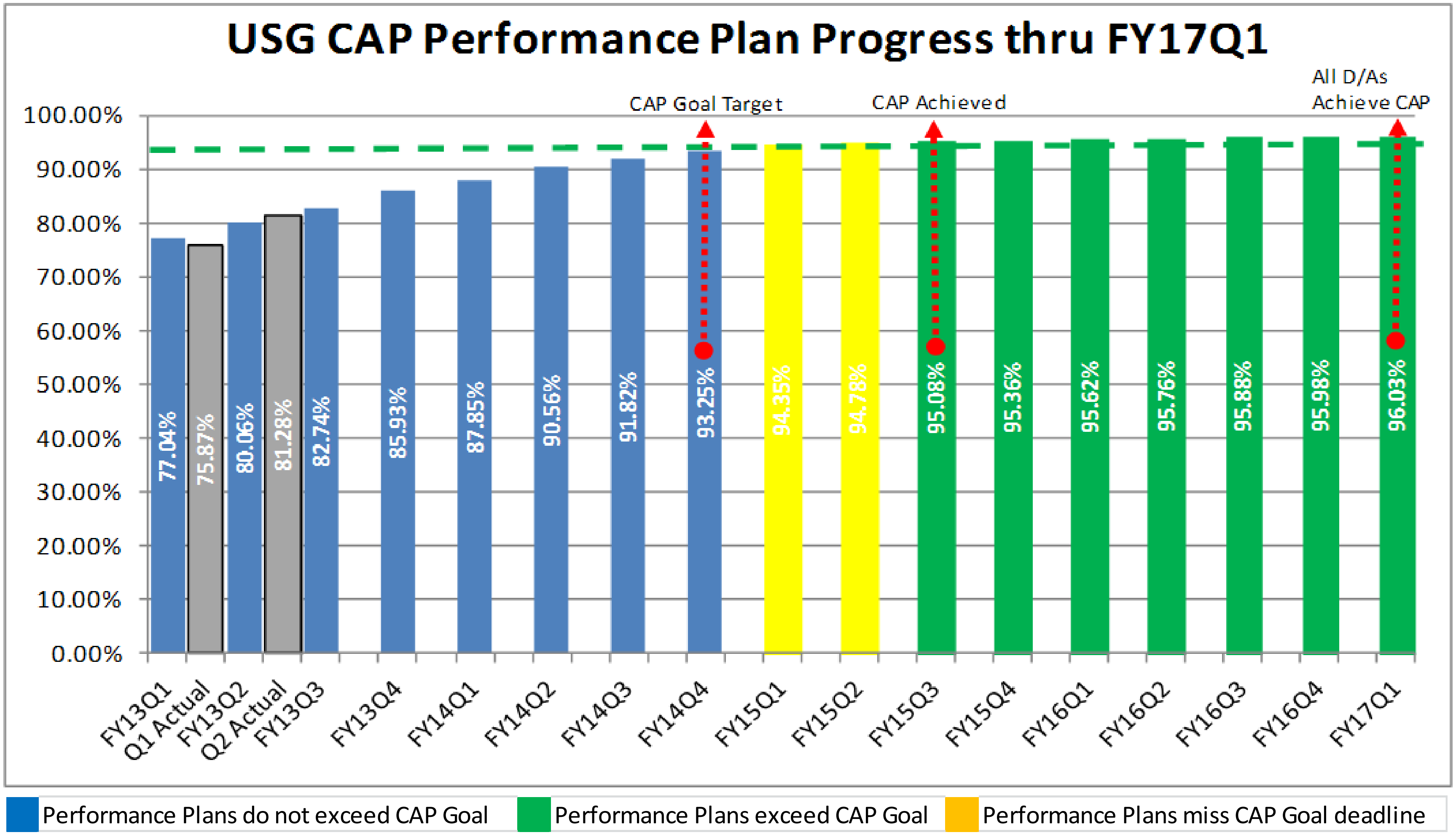
The next two charts show the progress towards the CAP priority cybersecurity capability goals across the government for the 24 Chief Financial Officer (CFO) agencies. The first chart shows the quarterly progress from Q1 FY13 to Q2 FY13.

Government-wide performance towards the Administration's Priority Cybersecurity Capabilities as of FY13 Q2



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.

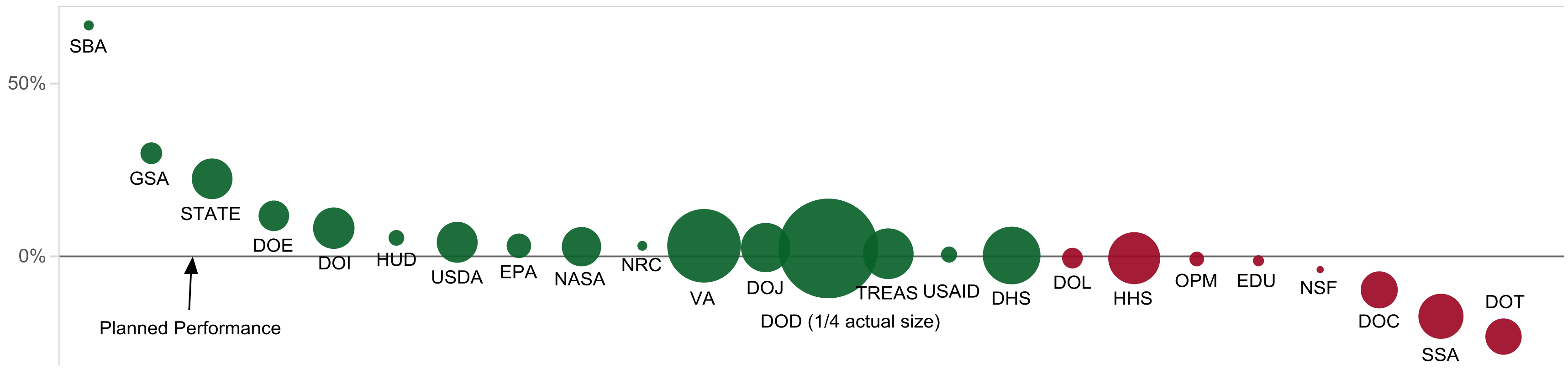
Government-wide performance towards the Administration's Priority Cybersecurity Capabilities



Agency Scorecards

Agencies are on separate tracks to reach the CAP goal targets for the priority cybersecurity capabilities. The graphic below shows which agencies are above or below their reported performance plans for FY2013 Q2. Agencies in green are above their planned performance plan for FY2013 Q2 and agencies in red are below. The Y-Axis indicates the percentage above/below planned performance. The relative size of the circle indicates the size of the number of assets and users representing the size of the agency.

Federal department and agencies above and below performance plan for FY2013 Q2



Federal department and agency performance for FY2013 Q1 – Q2 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.

	DOC				DHS				DOD				DOE				DOI				DOJ			
CAPABILITIES	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan
Continuous Monitoring	69	69	63	69	90	80	87	80	75	76	79	78	73	67	90	73	84	76	87	76	93	90	94	90
PIV Logical Access	19	19	18	20	18	19	21	29	84	90	92	90	2	0	4	0	19	11	30	15	7	6	13	15
TIC Traffic Consolidation	85	85	71	85	96	80	72	85	N/A	N/A	N/A	N/A	23	30	22	40	98	98	99	98	99	99	99	99
TIC 2.0 Capabilities (FY13)	70	70	74	80	80	80	87	85	N/A	N/A	N/A	N/A	88	85	88	85	90	90	77	92	98	98	98	98

	DOL				DOT				EDU				EPA				GSA				HHS			
CAPABILITIES	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan
Continuous Monitoring	94	93	91	92	60	68	52	73	93	93	95	93	59	37	64	45	95	95	93	93	79	87	87	89
PIV Logical Access	0	0	0	0	0	0	0	1	47	87	75	87	0	0	0	0	93	93	48	48	56	58	63	61
TIC Traffic Consolidation	83	83	100	100	91	95	91	95	80	80	80	80	95	95	95	95	70	70	100	73	0	0	0	0
TIC 2.0 Capabilities (FY13)	100	100	100	100	72	80	72	100	85	85	85	85	32	32	32	80	N/A	N/A	100	0	75	50	80	80

	HUD				NASA				NRC				NSF				OPM				SBA			
CAPABILITIES	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan
Continuous Monitoring	87	79	86	79	87	90	96	90	100	96	100	96	98	100	93	100	99	99	99	100	94	33	99	33
PIV Logical Access	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	26	8	4	8	0	0	0	0
TIC Traffic Consolidation	100	100	100	100	98	98	98	99	100	100	100	100	100	83	100	100	100	100	100	100	100	99	100	99
TIC 2.0 Capabilities (FY13)	68	68	68	69	87	88	87	88	100	100	100	100	100	100	100	100	92	92	92	92	100	100	100	100

	SSA				STATE				TREAS				USAID				USDA				VA			
CAPABILITIES	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan	Q1 FY13	Perf Plan	Q2 FY13	Perf Plan
Continuous Monitoring	69	87	82	92	67	48	76	48	82	82	80	80	100	98	99	98	69	79	100	100	98	95	100	95
PIV Logical Access	11	10	11	76	18	1	1	1	2	2	3	3	0	0	0	0	1	2	20	2	2	7	2	7
TIC Traffic Consolidation	100	100	100	100	100	96	100	96	95	95	95	95	100	100	100	100	100	100	100	100	19	19	19	19
TIC 2.0 Capabilities (FY13)	91	91	91	95	86	95	80	95	100	90	95	92	95	95	95	95	73	73	80	80	80	82	82	82

🟪🟪🟥🟥 Q2 < Performance Plan

→ Worse

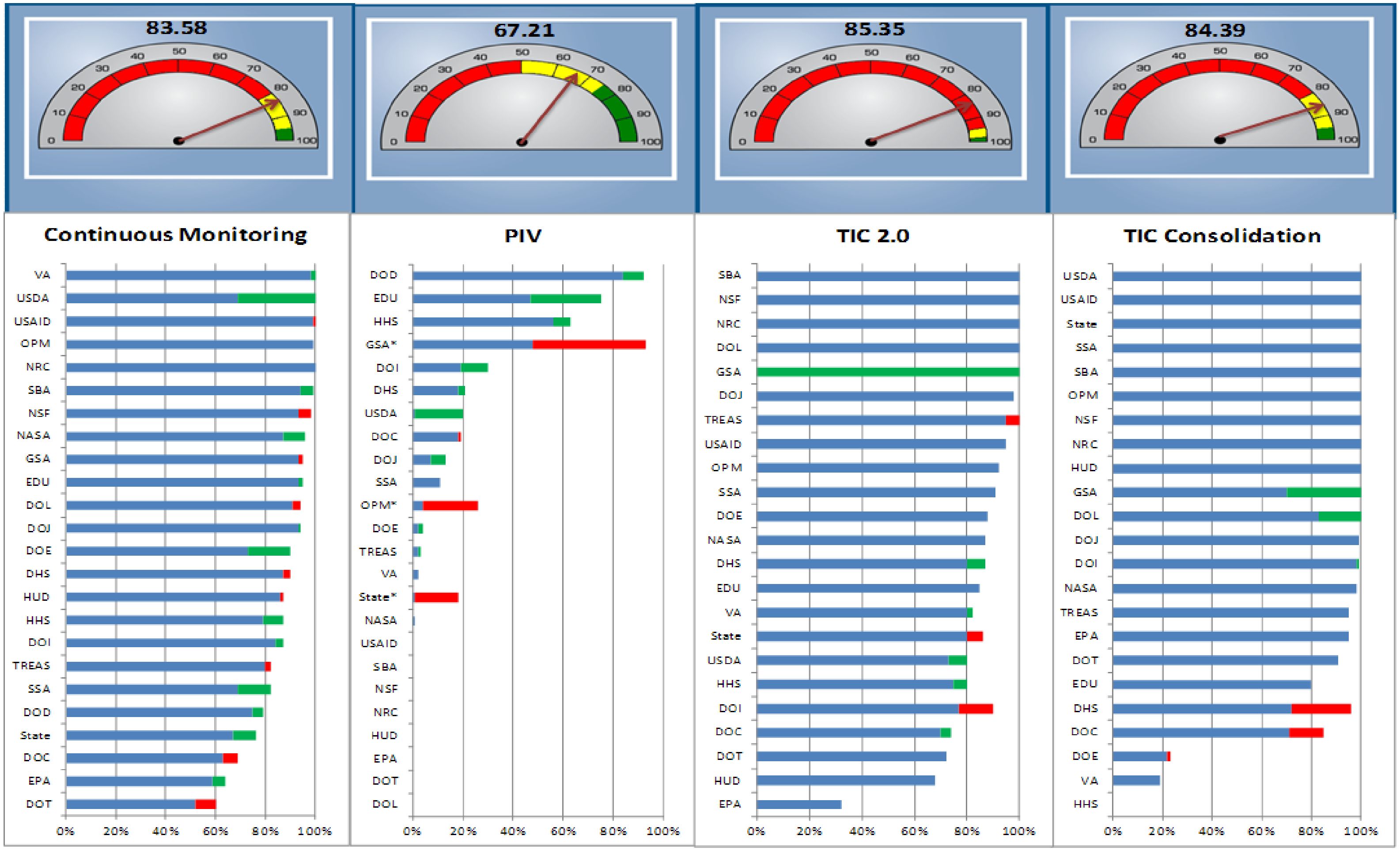
🟩🟩🟩🟩 Q2 => Performance Plan/Goal

→ Better

Federal department and agency performance for FY2013 Q1 – Q2

The chart below shows each agency's increase (green) or decrease (red) from FY2013 Q1 to Q2. 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.

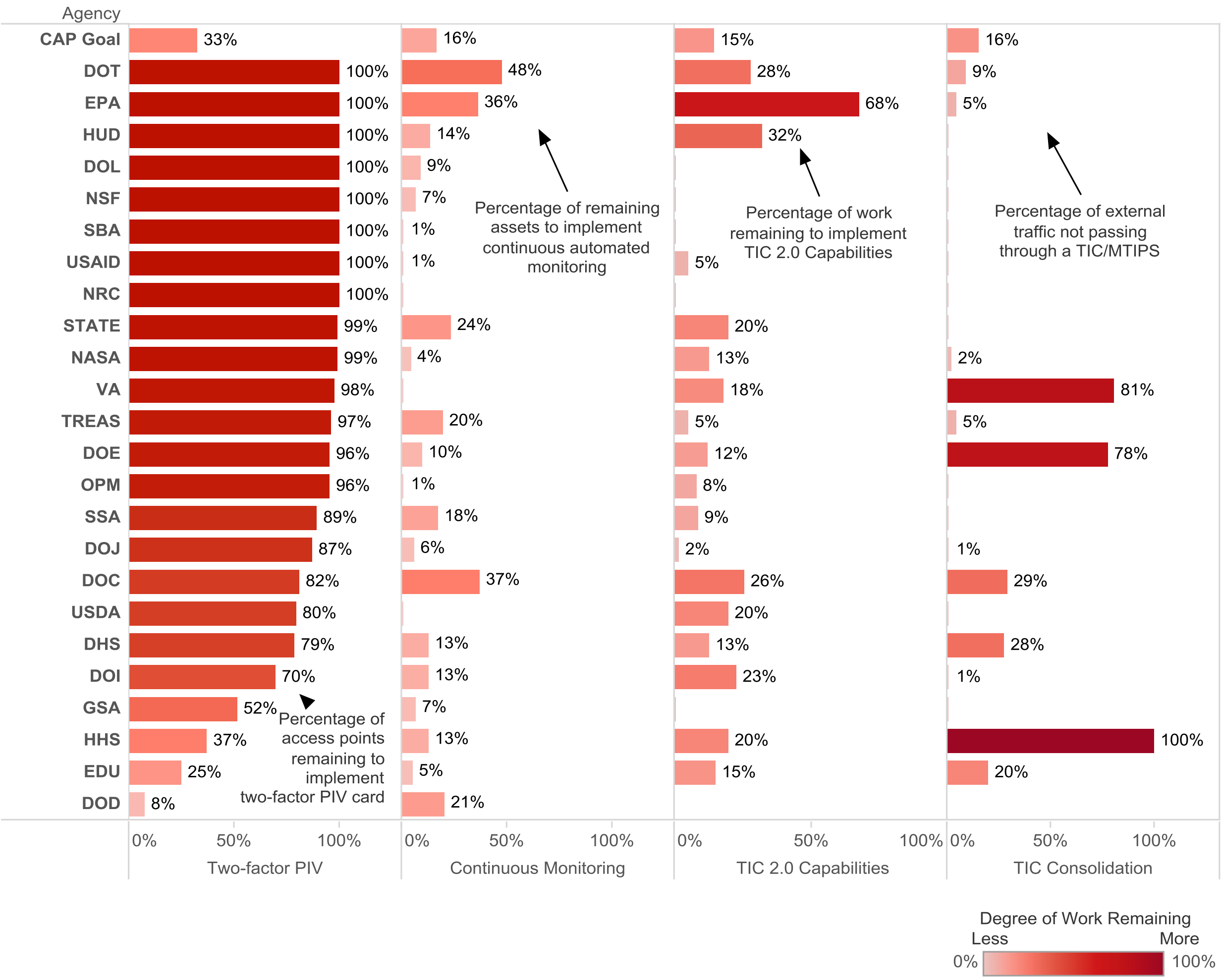
🟩 Q2 Increase from Q1 🟥 Q2 decrease from Q1



* Agency adjustment due to more accurate PIV reporting

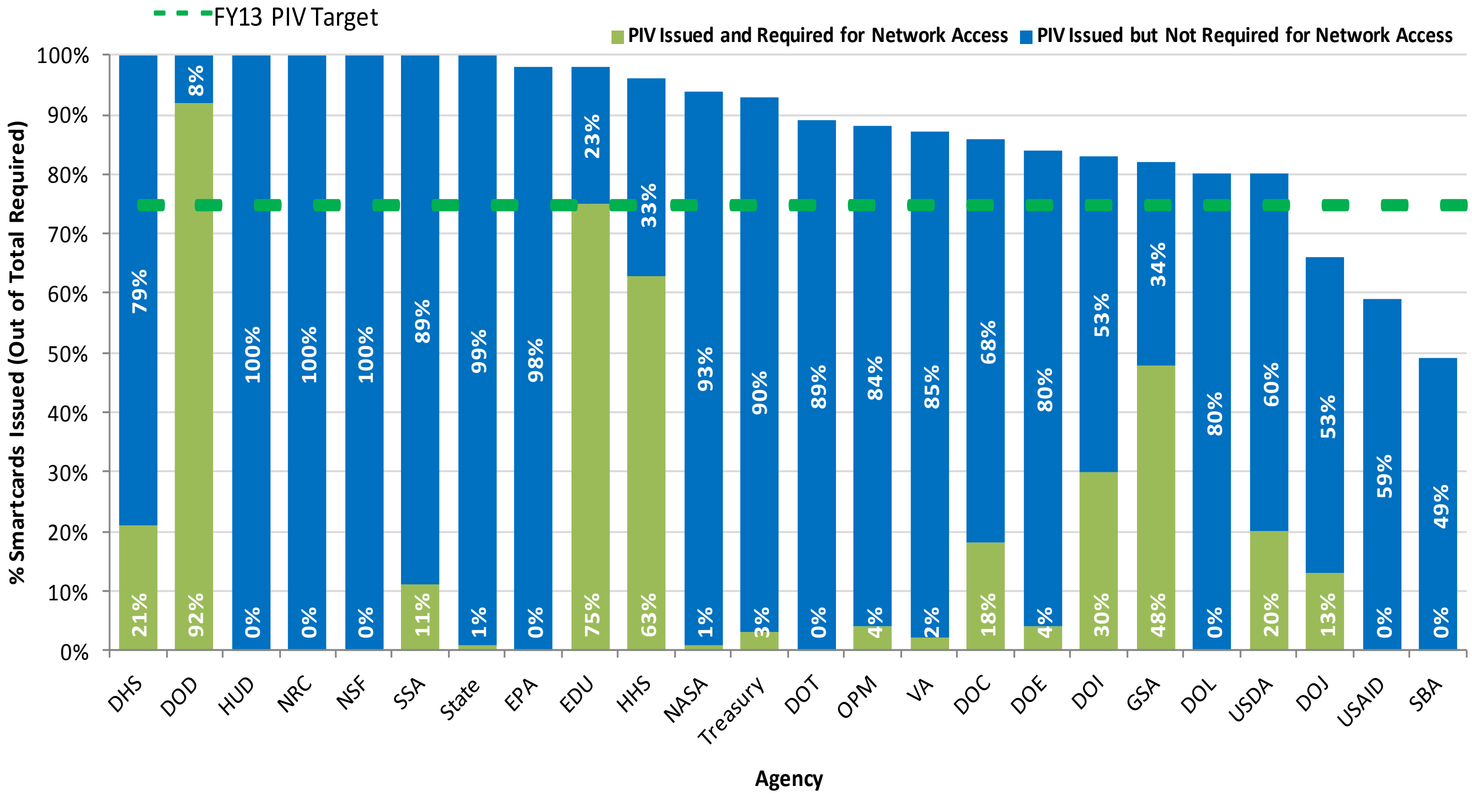
Work remaining

Much work remains for agencies to implement the Administration's priority cybersecurity capabilities. The following chart visually depicts how far each agency is from 100% implementation of each priority capability. Note this chart does not account for targets less than 100%.



Federal department and agency performance towards Strong Authentication with HSPD-12 Cards as of Q2 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%)

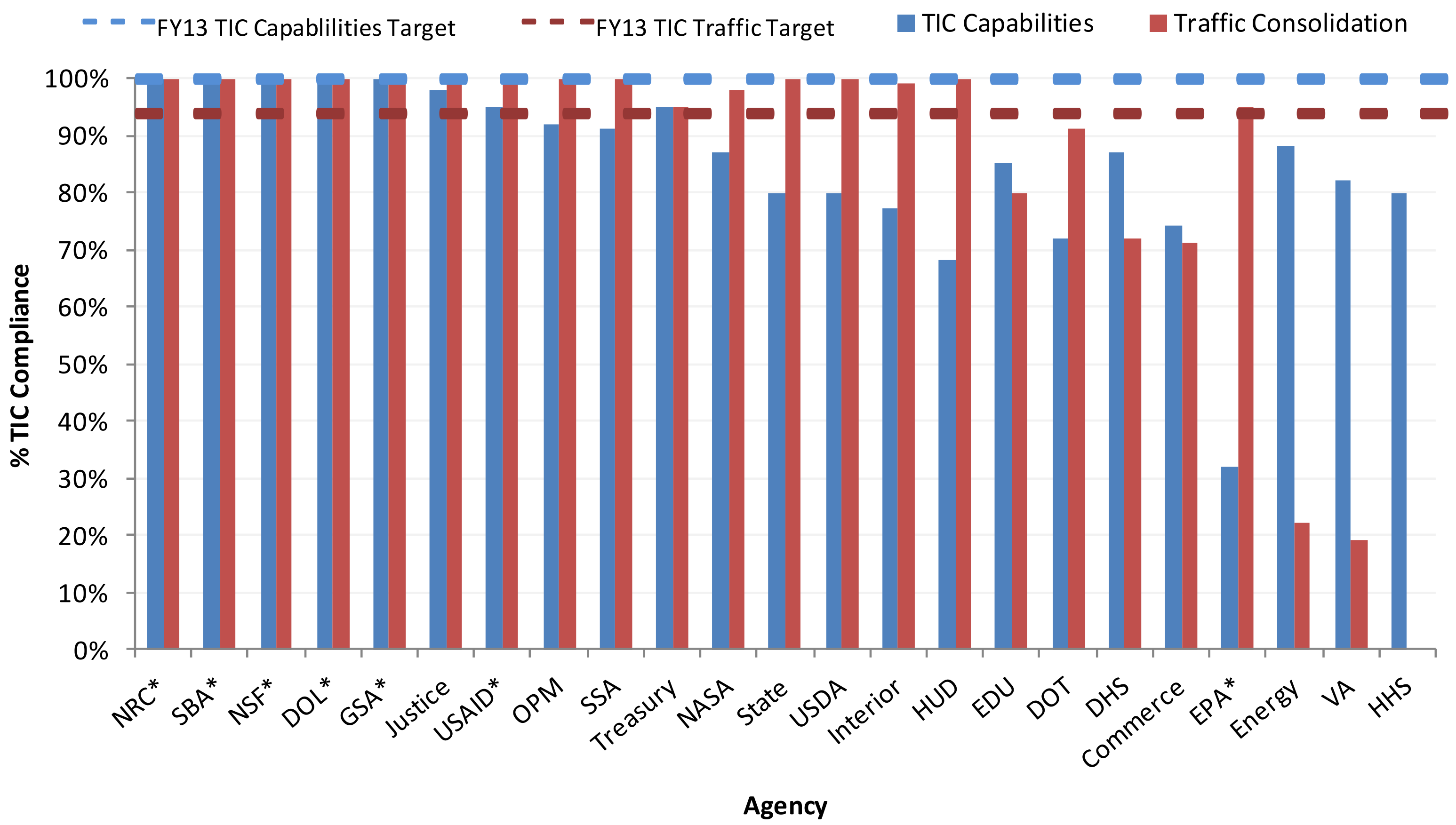
Percentage of accounts requiring use of PIV cards for network logon: 67%

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

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

The chart below shows the percentage of TIC traffic and TIC 2.0 capabilities at each agency as of Q2 FY2013.



TIC Capabilities represent TIC 2.0   * Agency uses MTIPS provider

TIC Capabilities: Agency FY13 target is 100% ; Government-wide status is 85% (increased 3% from FY13 Q1 to FY13 Q2)

TIC Traffic Consolidation: Agency FY13 target is 95%; Government-wide status is 84% (the same as in FY13 Q1)

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

[9] Section references are to the annual metrics only, and do not apply to the quarterly metrics.

[10] 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.

[11] Comprehensive National Cybersecurity Initiative (CNCI)

[12] Not applicable to Department of Defense (DOD).

Milestones Accomplished to Date (FY13Q2)

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**
- Develop a PIV Logical Access Control System (LACS) business case	**Completed**
- Develop a methodology and conduct PIV LACS-related cost and savings analysis	**Completed**
- Develop standard language for use by requiring officials in acquisitions to support PIV enablement and PIV compatibility and interoperability	**Completed**
- 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**