Cross Agency Priority Goal: Cybersecurity
FY2014 Q2 Status Update

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

Executive Summary

The federal government made progress toward the Administration's Priority Cybersecurity Capabilities over the past two quarters, with an overall increase in the capability adoption of 2.82%. While there was a decline in the mandatory HSPD-12 compliant PIV card use for strong network authentication, this was mainly attributable to a decrease in Department of Defense (DoD) personnel.

In FY14, all Chief Financial Officer (CFO) agencies were asked to provide an updated capability implementation plan for the Administration's priority cybersecurity capabilities through FY15. To date not all agencies have responded, and without the FY14 agency performance plans, predicting future achievements must rely on outdated FY12 performance plans. Despite the FY14 Q2 reporting that shows that agencies are making headway, the Federal government is still not on track to 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, however the practices of governance, risk management, and compliance in the domain of information security are youthful when compared to more mature business domains. The Federal government has enacted a number of policies and legislation aimed at defending and protecting 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 adequately protecting 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*

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.

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.[1]

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

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

(minimal adequate security). The agency head delegates the authority to ensure information security compliance to the Chief Information Officer (CIO).[2]

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. A common formulation for a performance framework has to do with budget, operations, and workforce. 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 Office of Management and Budget (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.[3]

Finally, these priority capabilities are to 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

[2] FISMA of 2002, Section 3544. Federal agency responsibilities
[3] 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 Security Content Automation Protocol (SCAP) data feeds provided to DHS. DHS in turn analyzes the SCAP data along with other data sources to provide performance information to OMB, Department of Homeland Security (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 –** The application of security controls is prescriptive in 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 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[4] and the same FISMA metrics and operational guidance provided by DHS.

Progress reporting should be no less than quarterly as required under GPRA Modernization.[5] 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.

Lessons Learned

DHS is continually working to improve the capabilities aimed at addressing the cyber risk associated with Federal information systems. These on-going efforts enhance the Department's ability to protect the Federal Executive Branch civilian networks and further improve the overall cybersecurity environment. Each of the existing cyber cap goals provides distinct lessons learned that inform future planning:

> **Information Security Continuous Monitoring –** Situational awareness of security posture in near-network time is essential to protect systems against modern threats and adversaries. Security operators need the real-time security status of their systems, and management needs up-to-date assessments in order to make data driven risk-based decisions. ISCM provides the required near-network time view into security posture, and has become a key focus point for improving Federal information security.

[4] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf

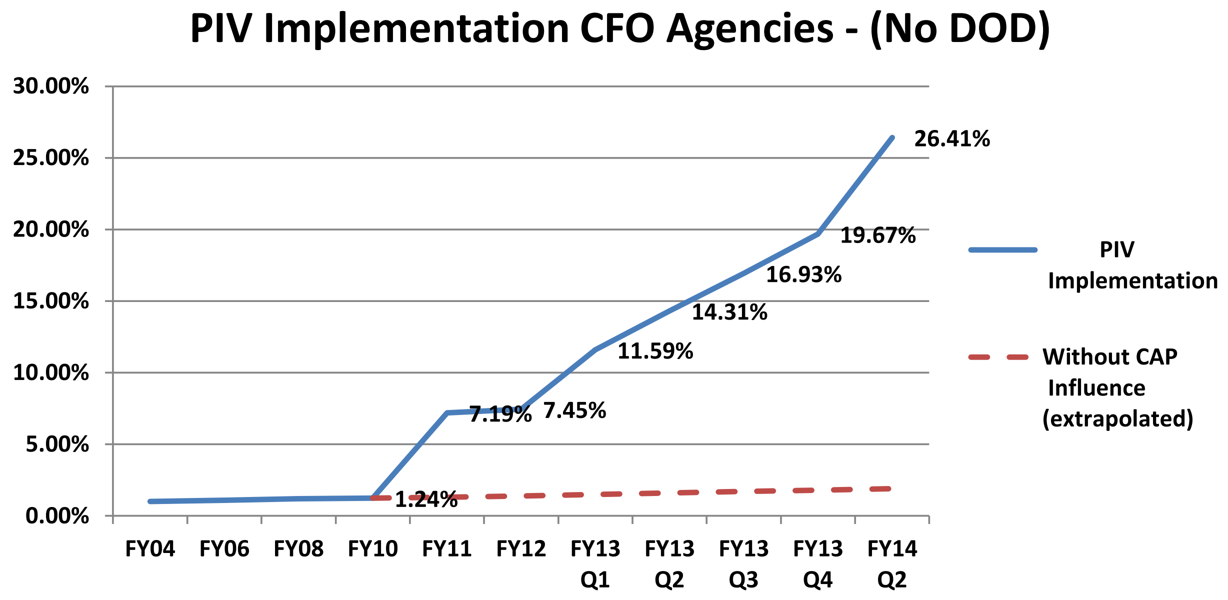
[5] As stated in the GPRA Modernization Act of 2010 Sec. 1121. *Quarterly priority progress reviews and use of performance information*, the cybersecurity CAP Goal progress will be reviewed to assess whether agencies are making progress towards milestones as planned.

At the level of the Federal enterprise, the current CAP metrics fail to provide adequate situational awareness as to where agencies stand with implementing and operating continuous monitoring as it is envisioned by NIST SP 800-137 and OMB M-14-03, DHS Continuous Diagnostics and Mitigation (CDM) ConOps, and the ISCM ConOps.

In the context of Enterprise Architecture and Governance, it is helpful to consider continuous monitoring in light of the following question: Is the right data getting to the right decision makers in a timely, reliable, and actionable manner? Moving forward, with the benefit of improved specificity and guidance, the meaningful measurement of continuous monitoring must include both the constituent capabilities specified by ISCM/CDM, but must also look at the degree of implementation and the alignment between policy, processes, and tools.

Through the CDM program, 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.

Personal Identity Verification (PIV) - Strong Authentication, the implementation of the HSPD-12 directive and the PIV specification, is an area that benefited significantly from CAP Goal status. Despite HSPD-12 having been a directive since 2004, Federal Civilian Government adoption of PIV prior to 2011, beyond simply issuing cards, was almost non-existent. During the period-of-performance for the CAP goals, there is a significant positive trend in PIV adoption. This trend is clearly related to the attention to the issue that comes with being included as a CAP goal.



An important lesson learned in the PIV domain concerns the current practice of exclusively measuring outcomes. Asking *how many users are required to use PIV for authentication* fails to measure, identify, or even consider underlying implementation issues. Despite positive trends in adoption, we find that there is cause for concern in the underlying numbers.

Because DoD is larger than the rest of the Federal workforce combined, along with the DoD's high scores on mandatory PIV usage, as DoD undergoes reductions in the workforce, so are the chances of the Government reaching the PIV goal of 75% reduced proportionately.

Despite steady progress toward achieving a 'passing' PIV mark for organizations in FY14, the *mode average*, that is the *outcome that is most likely to be observed*, stands at zero.

With so many agencies struggling to get a foothold on PIV implementation DHS and OMB, we will introduce measurements in FY15 for PIV performance that include implementation and maturity related metrics. By measuring and monitoring progress with planning, resource commitments, and acquisition related activities, the Federal Enterprise will be able to realize the fullest intent of the CAP program by facilitating cross agency collaboration to overcome constraints and barriers to PIV implementation.

Trusted Internet Connections - The purpose of the TIC initiative is to improve the Federal government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections. This is accomplished by establishing TIC Access Providers (TICAP) and Managed Trusted Internet Protocol Services (MTIPS) providers. Each TICAP and MTIPS provider has baseline security capabilities including firewalls, malware policies, and network/security operation centers. The National Cybersecurity Protection System (NCPS) EINSTEIN 2 capability is also deployed at each access point. EINSTEIN 2 is an Intrusion Detection System (IDS) capability that alerts when a specific cyber threat is detected. This allows The United States Computer Emergency Readiness Team (US-CERT) to analyze malicious activity occurring across the Federal IT infrastructure resulting in improved computer network security situational awareness.

The next iteration of the EINSTEIN capabilities is designed to include an intrusion prevention capability (previously referred to as EINSTEIN 3). The intrusion prevention capability (IPS) builds upon the previous versions by adding the ability to block and disable attempted intrusions before any harm is done. In 2012, DHS transitioned the approach of the EINSTEIN 3 program from one in which the government builds and deploys intrusion prevention systems to one in which DHS contracts with major Internet Service Providers (ISPs) to supply intrusion prevention security services as a managed security services offering. These services are then augmented through the sharing of sensitive government information with those service providers. This accelerated program is called EINSTEIN 3 Accelerated, or E3A.

The transition to E3A represents a smarter, stronger, faster way to achieve the goals of delivering an intrusion prevention capability. E3A leverages private sector cybersecurity innovation enhanced by data that is uniquely held by the Federal Government. The initial deployment of E3A is focused on countermeasures that will address 85% of the cybersecurity threats affecting the Federal Executive Branch civilian networks, in a fraction of the time required by the original EINSTEIN 3 government-furnished equipment approach.

In March 2013, DHS awarded its first ISP contract for E3A services. This contract award was the first step in the rollout of capabilities that will protect the Federal Executive Branch civilian networks under E3A. For FY14, DHS Network Security Deployment (NSD) will continue with the rollout of E3A and securing the IPS Memorandums of Agreement (MOAs) with all departments and agencies. Progress with consolidating traffic across all CFO Act D/A's and the move to managed security services offerings indicates that implementation issues are well understood and mechanism and resources are in place for monitoring and supporting the TIC directive. As a result, TIC will no longer be a focus of the CAP Goal, but will remain an Administration focus and all Departments and Agencies are expected to continue to fully implement it as part of their network architecture.

CAP Goals for FY15/17

In August 2013, The National Security Staff convened the Joint FY15 Working Group. The group was tasked with developing the future CAP goal priorities and objectives. The group selected the following priorities:

- Information Security Continuous Monitoring (ISCM/CDM)
- Phishing and Malware Defense
- Identity, Credential, and Access Management (ICAM/PIV)

DHS, with the final outputs of the J15 working group, is developing these focus areas into three sets of operational metrics. These metrics will have traceability to statutory requirements, and are intended to measure the wide array of activities that compose ISCM/CDM, anti-phishing, and ICAM activities.

Based on lessons learned from the 12/14 Interim Goals, it is the intention of DHS that a scoring methodology be employed that scores both implementation and performance factors. In addition, where there are multiple possible, but not mandated, solutions such as Phishing and Malware Defense, a scoring methodology be developed that recognizes different, but valid, approaches.

After developing a comprehensive set of metrics for each priority area, DHS will develop a factored scoring scheme, applying a weighted score to each individual factor. The factors will be identified through consultation with Government and Industry partners and validated through interagency working groups. In a factored scoring scheme, new factors can be added, or weighted differently, with manageable changes to the expressed score. The scoring factors will be under a change management process to regulate their priority, impact, and weight. Previously by exposing the raw reported results, changes in requirements, as occurred with TIC, caused significant variations in the scoring.

As these metrics represent new data gathering, DHS does not have an accurate trend or established baseline of performance across Federal departments and agencies. The remainder of FY14 will be spent establishing a baseline of performance for the new CAP goal priorities areas before beginning to track performance and set goals for FY15 and beyond. With input from NSS, OMB, and interagency committees, DHS will utilize qualitative measurements and quantitative statistical modeling, to include data sampling, to analyze data from FY14 and establish achievable target performance for FY15 and beyond.

ISCM/CDM

Continuous Monitoring is carried over as a goal with additional metrics related to implementation, maturity, and compliance with OMB 14-03.

ICAM

PIV is carried over as a goal with additional metrics related to implementation, and maturity.

Phishing and Malware Defense

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as data theft, terrorism, foreign intelligence-gathering and acts of war. The sophistication and effectiveness of cybersecurity attacks have steadily advanced. These attacks often take advantage of flaws in software code, use exploits that can circumvent signature-based tools that commonly identify and prevent known threats, and employ social engineering techniques designed to trick the unsuspecting user to click a malicious link or open a malicious attachment thereby giving an attacker direct access onto the Government network.

Advances in anti-phishing measures have caused attackers to increase the sophistication of their techniques to bypass detection. The frequency and sophistication of phishing attacks have increased, and spyware has proven to be difficult to detect and remove.

US-CERT receives computer security incident reports from the Federal Government, State/Local governments, commercial enterprises, U.S. citizens and international Computer Security Incident Response Teams (CSIRTs).[6] The total number of incidents for each group can be found in Table 1 below.

Table 1. Incidents Reported to US-CERT in FY 2012 - FY 2013

Reporting Source	Total Number of Incidents FY12	Total Number of Incidents FY13
Federal Government Total	48,842	60,753
Federal Government: CFO Act	46,043	57,971
Federal Government: Non-CFO Act	2,799	2,782
Other (State, Local, Tribal Governments and Commercial)	104,201	158,133
TOTAL	153,043	218,886

The total number of reported incidents impacting the Federal Government increased by approximately 24% from FY 2012 while the number of reported incidents from all sectors combined increased by approximately 43% for the same period.

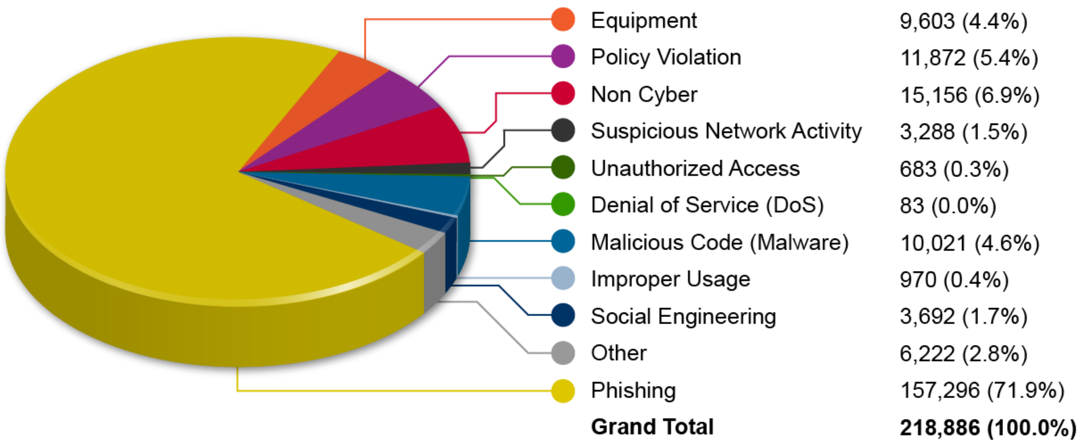
For FY 2013, US-CERT processed 218,886 incidents as categorized in Figure 2.[7] Phishing, a type of social engineering, which is reported voluntarily to US-CERT by private individuals and organizations, continues to be the most widely reported incident type. As indicated in

[6] A computer security incident, as defined by NIST Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

[7] For more information, refer to the US-CERT website at: http://www.us-cert.gov/.

Figure 1, which includes a breakout of all incidents reported to US-CERT in FY 2013, phishing accounted for 71.86% of total incidents reported.

Figure 1. Summary of Total Incidents Reported to US-CERT in FY 2013



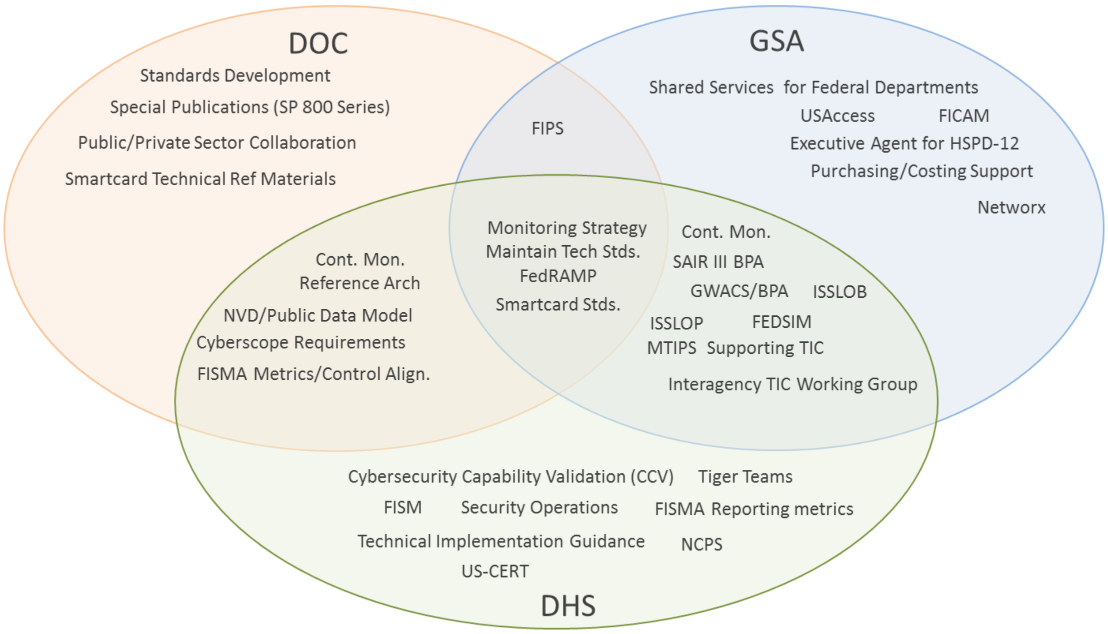
Due to the preponderance of phishing attacks and their steadily increasing frequency, malware protection will be added as a CAP goal beginning in FY15. US-CERT and NSA both identified phishing as one of the top threat vectors putting Federal Departments and Agencies at risk. Consistent with the other FY15/17 CAP Goals, metrics are being developed to appropriate measure Department and Agency performance in addressing the phishing and malware threat.

Major Activities (FY2014 Q2-3)

Activity	Status
FY 15 CIO Metrics - DHS, Federal Network Resilience (FNR), is engaged broadly with Federal cybersecurity workforce members in the development of the FY 15 CIO Metrics.	Metrics on track for June, 2014 delivery to OMB. Future planning sprints are in the works for IG and IC communities. In Q4FY14.
NCCIC/USCERT will publish new Incident Reporting guidance, conformant with NIST 800-61r, intended to produce more actionable and measurable outcomes.	NCCIC/USCERT is working with DHS FNR to socialize changes, produce guidance, and identify early adopters.

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 Department of Commerce (DOC) 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 interim priority cybersecurity capabilities and reported progress through the FY2011 FISMA report[8], and continued with the FY2012, FY2013, and FY2014 FISMA metrics[9]. 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 FY2014 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**							
	FY2012Q4	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q4	FY2014Q2	FY2013Q1	FY2013Q2	FY2013Q3	FY2013Q4	FY2014Q1	FY2014Q2	FY2014Q3	FY2014Q4
Continuous Monitoring	79.53%	78.42%	83.58%	82.07%	81.01%	85.46%	78.68%	81.27%	82.05%	85.13%	87.57%	90.19%	91.74%	94.93%
Strong Authentication	57.26%	53.72%	67.21%	66.70%	66.61%	62.81%	61.07%	65.71%	67.25%	75.41%	76.20%	70.92%	74.21%	78.91%
TIC Consolidation	81.22%	84.00%	84.39%	84.17%	86.43%	90.00%	84.00%	86.48%	89.13%	91.61%	93.09%	91.87%	93.52%	94.43%
TIC Capabilities	83.87%	82.21%	85.35%	83.78%	87.48%	91.26%	80.96%	84.96%	90.26%	92.13%	92.74%	93.30%	94.61%	96.48%
Overall Cyber CAP	76.82%	75.87%	81.28%	80.14%	80.59%	83.41%	77.01%	80.16%	82.13%	85.76%	87.46%	87.77%	89.59%	92.43%

Table 1: Cybersecurity CAP Quarterly targets

[8] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11__e-gov_act_report.pdf

[9] http://www.dhs.gov/xlibrary/assets/nppd/ciofismametricsfinal.pdf

Progress Update[10]

The FY2014 Q2 FISMA reporting showed moderate progress this quarter in the overall Administration's priority cybersecurity capabilities. A decrease in strong authentication tempered solid advances in the areas of continuous monitoring and TIC compliance. Although there was only moderate progress, the solidity and accuracy of the reporting foundation seems to be continually improving. The chart below represents the results of the quarterly FISMA reporting for FY2013 Q4 and FY2014 Q2 for the Administration's priority cybersecurity capabilities.

	USG-Wide Quarterly Results		FY14 Targets
	FY2013 Q4	FY2014 Q2	Target FY2014
Continuous Monitoring	81.01%	85.46%	95%
Strong Authentication	66.61%	62.81%	75%
TIC Consolidation	86.43%	90.00%	95%
TIC Capabilities	87.48%	91.26%	100%
Weighted Average	80.59%	83.41%	93%

FISMA Metrics

The previous reporting quarter, FY2013 Q4, only saw improvement in the capability area of TIC compliance although this was enough to advance the overall CAP score ever so slightly. This quarter significant gains were also seen in the continuous monitoring capability, propelling the overall CAP score to its largest gain in the last four quarters. Once again, the fluctuating nature of DOD personnel greatly influenced strong authentication. As DOD reported fewer personnel, the majority of whom were mandatory PIV users, the government-wide implementation of strong authentication decreased. This was even as many of the other CFO agencies reported excellent strides towards the PIV implementation goal. Eventually, as the other CFO agencies achieve more substantial implementation of the cybersecurity capabilities, DOD will have less and less influence on the overall percentages. However, for the near future DOD will continue to drive the numbers for continuous monitoring and strong authentication.

[10] Due to the lapse in appropriations, the data call for FY13 CIO Metrics did not close until December 2013. Based on a suggestion from a meeting of the Security Program Management sub-committee of the Information Security and Identity Management Committee (ISIMC), the Q1FY14 data call did not occur. Community members were concerned that an identical data call for the CAP metrics following so closely would not produce meaningful results. After consultation between DHS, OMB, and NSCS it was decided that, a January data call would be redundant in nature and provide little additional value beyond the previously reported metrics.

Continuous monitoring increased over four percent even as one-half of the CFO agencies reported an increase in discovered assets while the other half reported a decrease. The majority of the increases or decreases were slight in number with a few exceptions. The Department of Agriculture (USDA) reported more than twice the number of previously reported assets, which in turn dropped their asset management score by more than half. While the continual maturation of the asset discovery process leads to increased asset counts, which may temporarily depress scores (jitter), it also leads to a more accurate foundation for future accounting.

Overall, however, FY14 Q2 resulted in a 13% decrease in the number of assets reported government-wide, as DOD reported well over a million less assets. DOD has streamlined its asset reporting in FY14 in order to better leverage their automated tools and provide increased consistency in reporting across the Department. Asset types included in their reporting are network devices, physical desktop computers, laptop computers, physical servers, and virtual servers. By tailoring their reporting to a normalized set of assets DOD now comprises 41% of government assets as opposed to the 51% previously, which reduces the significant effect DOD has historically had on the overall government-wide numbers. Outside of DOD, the other CFO agencies reported an increase of 175,000 assets in FY14Q2.

Strong authentication declined in FY14Q2 as DOD continues to influence the PIV implementation percentage with its personnel fluctuations. This quarter DOD reported more than half a million less PIV users than last quarter. Without DOD, the other 23 CFO agencies would have added over 122,000 PIV users and increased their PIV implementation by 6.74%. National Aeronautic and Space Administration (NASA) [27%], DHS [14%], and DOC [12%] saw double-digit gains, while Department of the Interior (DOI) and National Science Foundation (NSF) finally began implementation.

The TIC 2.0 Capabilities metric increased 3.78% as six agencies made advances and fifteen agencies remained the same as last quarter. The greatest improvements were from Department of Housing and Urban Development (HUD) and DOC which improved 30% and 27% respectively. Gains were seen in TIC Traffic Consolidation as four agencies improved and only one agency reported a decrease. The best increase was from Department of Health and Human services (HHS), which improved from 0% to 61% for traffic consolidation. Seventeen of the twenty-three CFO agencies have achieved the CAP goal of 95% for TIC Traffic Consolidation and fifteen agencies now report a score of 99% or better.

FY2013 Q4 Summary

- The overall Cyber CAP score increased by 2.82% from FY13 Q4 to FY14 Q2 as gains in the implementation of priority cybersecurity capabilities were realized in all but one capability area.

  - The overall Continuous Monitoring score increased 4.45% as agencies reported increases in automated asset management, automated configuration management, and automated vulnerability management.
  - TIC 2.0 Capabilities increased 2.52% and TIC Consolidation increased 4.83% as agencies continued to migrate to the TIC 2.0 architecture.
  - Strong Authentication decreased 3.80% as gains by the CFO agencies were offset by a reduction in PIV enabled DOD personnel.
- Continuous Monitoring
  - Government-wide (USG), the Automated Asset Management score rose 6.30% and now stands at 89.40%. Twenty agencies have reached the minimum target of 80% for Automated Asset Management and fourteen have reached or exceeded the goal of 95%.
  - Automated Vulnerability Management increased 6.38% as previously unmanaged assets came under management.
  - Automated Configuration Management had a slight increase of 0.68% and remained the most challenging aspect of continuous monitoring.
  - Agencies deemed on average that 75% of assets were applicable to Configuration Management while six agencies reported on all assets for Configuration Management.
- Strong Authentication
  - In FY14 Q2 the CAP score for strong authentication fell by 3.8%.
  - DOD reported 568,000 less PIV users as its workforce continues to fluctuate.
  - Without DOD, the USG PIV implementation score for the other 23 CFO agencies would have risen 6.74% as 122,000 more users were required to use PIV cards to access the network.
  - More than half the CFO agencies (13) are now in double digit PIV implementation percentages.
  - Eight (8) agencies still remain at 0% for PIV implementation and another three (3) are at 3% or less.
  - DOD, GSA, and Social Security Administration (SSA) are the only agencies reporting at or above the FY2014 goal of 75%.
  - HHS and Department of Education (EDU) are reporting above the FY14 FISMA minimum of 50% and DHS, DOC, and NASA have reached the 40% plateau.
- Trusted Internet Connection (TIC)
  - The Government-wide implementation of TIC 2.0 Capabilities now stands at 91.26% and TIC Traffic Consolidation at 90.00%.

- Eighteen of the 23 CFO agencies (DOD is exempt from this reporting) achieved the minimum FY 13 FISMA target of 80% consolidation with 17 reaching the CAP goal of 95%.
- Department of Energy (DOE), Department of Veterans Affairs (VA), HHS, USDA and DOC remain below the TIC Consolidation minimum.
- HUD improved their TIC 2.0 Capabilities from 68% to 98%
- HHS improved their TIC Consolidation from 0% to 61%

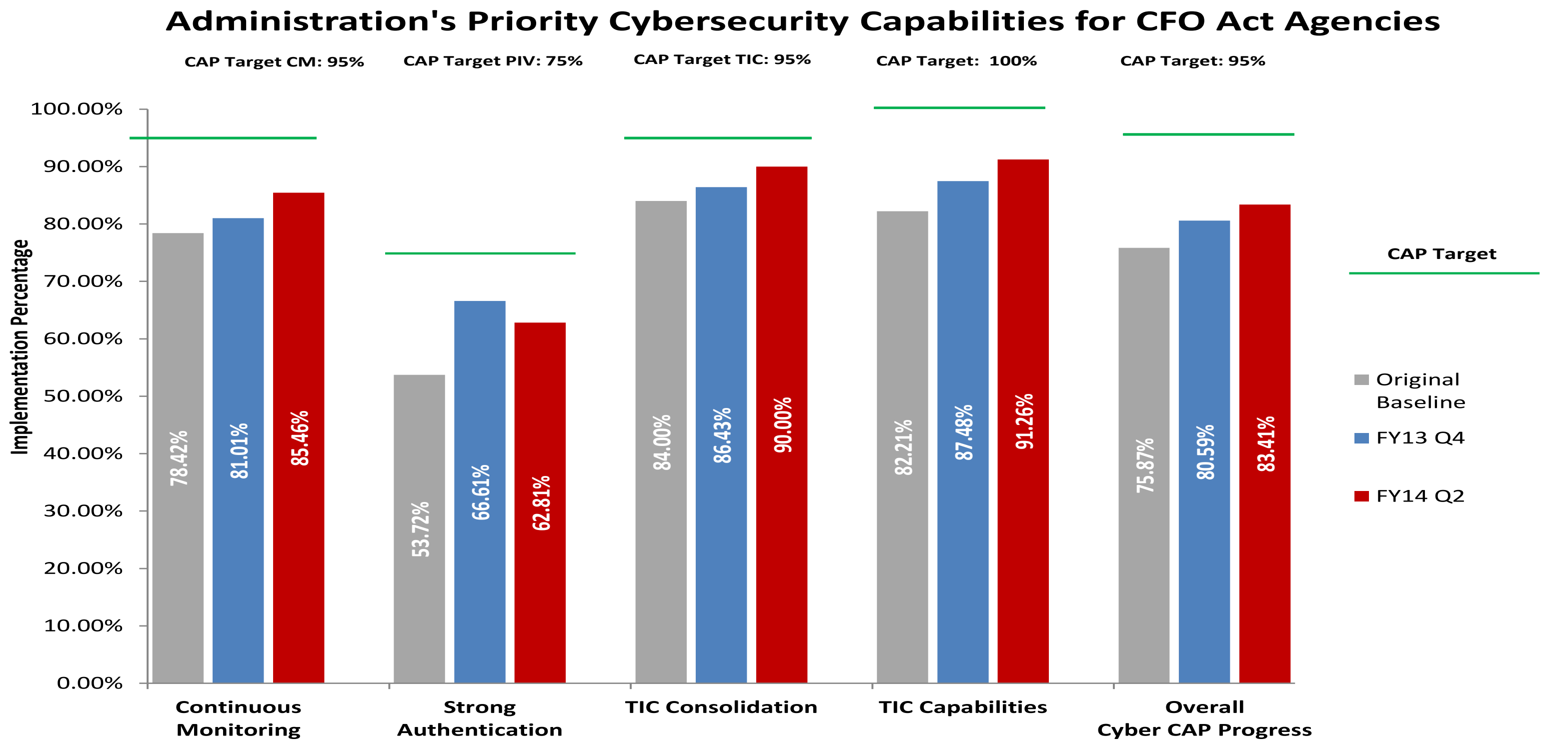
Scorecards

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 FY2014 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.

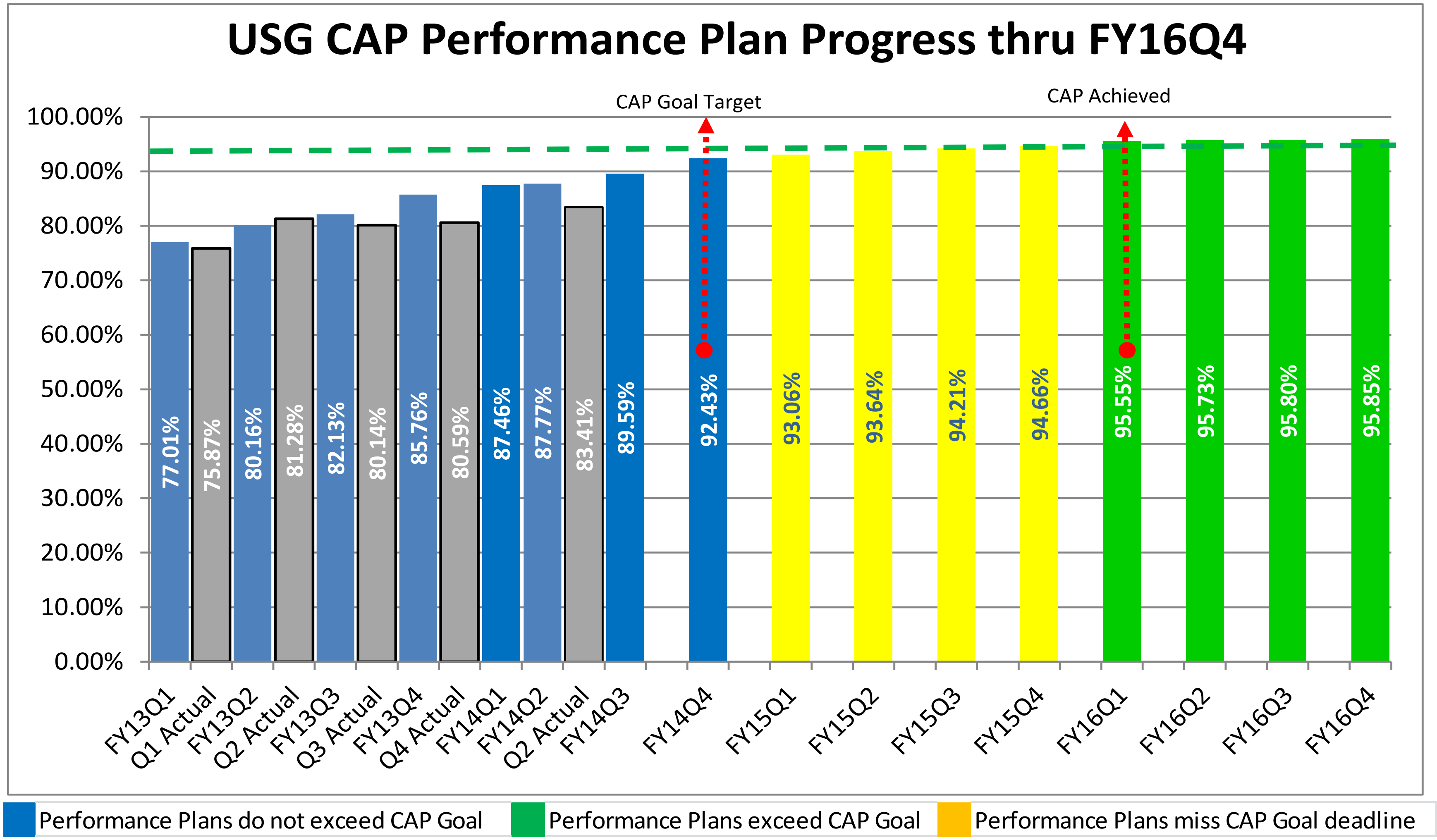
Government-wide Scorecards

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 Q4 FY13 to Q2 FY14.

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



Government-wide performance towards the Administration's Priority Cybersecurity Capabilities as of FY14 Q2
The chart below shows the actual FY14 Q2 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 FY14 Q4 based on the agency performance plans.



Federal department and agency performance for FY2013 Q4 – FY2014 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 planed and actual performance improvement.

	DOC				DHS				DOD				DOE				DOI				DOJ			
CAPABILITIES	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14
Continuous Monitoring	73	69	95	72	90	94	85	88	83	76	88	85	80	86	90	92	87	86	87	87	92	99	99	88
PIV Logical Access	24	30	30	42	49	30	43	44	94	89	91	81	73	9	29	14	15	0	50	0	50	30	33	29
TIC 2.0 Capabilities	85	41	90	68	95	92	92	92	N/A	N/A	N/A	N/A	95	92	95	92	100	86	100	85	98	93	93	93
TIC Traffic Consolidation	86	76	92	76	95	94	95	95	N/A	N/A	N/A	N/A	60	26	55	46	99	99	99	99	99	99	100	100

	DOL				DOT				EDU				EPA				GSA				HHS			
CAPABILITIES	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14
Continuous Monitoring	99	97	98	99	51	52	60	79	93	95	97	90	47	57	55	55	95	98	98	98	91	90	92	95
PIV Logical Access	18	0	35	0	2	7	10	13	89	75	90	72	2	0	0	0	94	94	94	94	69	66	75	68
TIC 2.0 Capabilities	100	100	100	100	70	72	70	89	85	85	90	85	83	90	90	90	100	100	98	98	100	100	100	100
TIC Traffic Consolidation	100	100	100	100	95	99	95	99	80	91	80	91	100	95	95	95	100	100	100	100	75	0	90	61

	HUD				NASA				NRC				NSF				OPM				SBA			
CAPABILITIES	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14
Continuous Monitoring	91	85	93	89	92	88	97	95	96	95	89	88	100	95	100	96	100	97	97	97	52	63	67	100
PIV Logical Access	0	0	49	0	20	17	29	44	0	0	9	0	0	0	2	4	51	0	0	0	50	0	0	0
TIC 2.0 Capabilities	69	68	95	98	89	88	88	88	100	100	99	100	100	100	100	100	100	82	90	88	100	100	100	100
TIC Traffic Consolidation	100	100	100	100	100	100	100	100	100	100	95	100	100	100	100	100	100	100	100	100	100	100	99	99

	SSA				STATE				TREAS				USAID				USDA				VA			
CAPABILITIES	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14	Perf Plan	Q4 FY13	Perf Plan	Q2 FY14
Continuous Monitoring	95	96	95	97	87	82	92	87	75	84	93	95	100	97	100	97	100	99	100	81	95	77	95	78
PIV Logical Access	75	85	75	86	6	1	5	1	38	9	13	14	0	0	0	0	50	6	65	3	6	0	6	13
TIC 2.0 Capabilities	95	96	95	96	90	78	78	78	93	93	96	95	100	92	100	100	90	82	95	82	82	82	92	82
TIC Traffic Consolidation	100	100	100	100	100	100	100	100	99	99	99	99	100	100	100	100	100	71	100	71	19	39	19	39

🟪🟪🟥🟥 FY14Q2 < Performance Plan

→ Worse

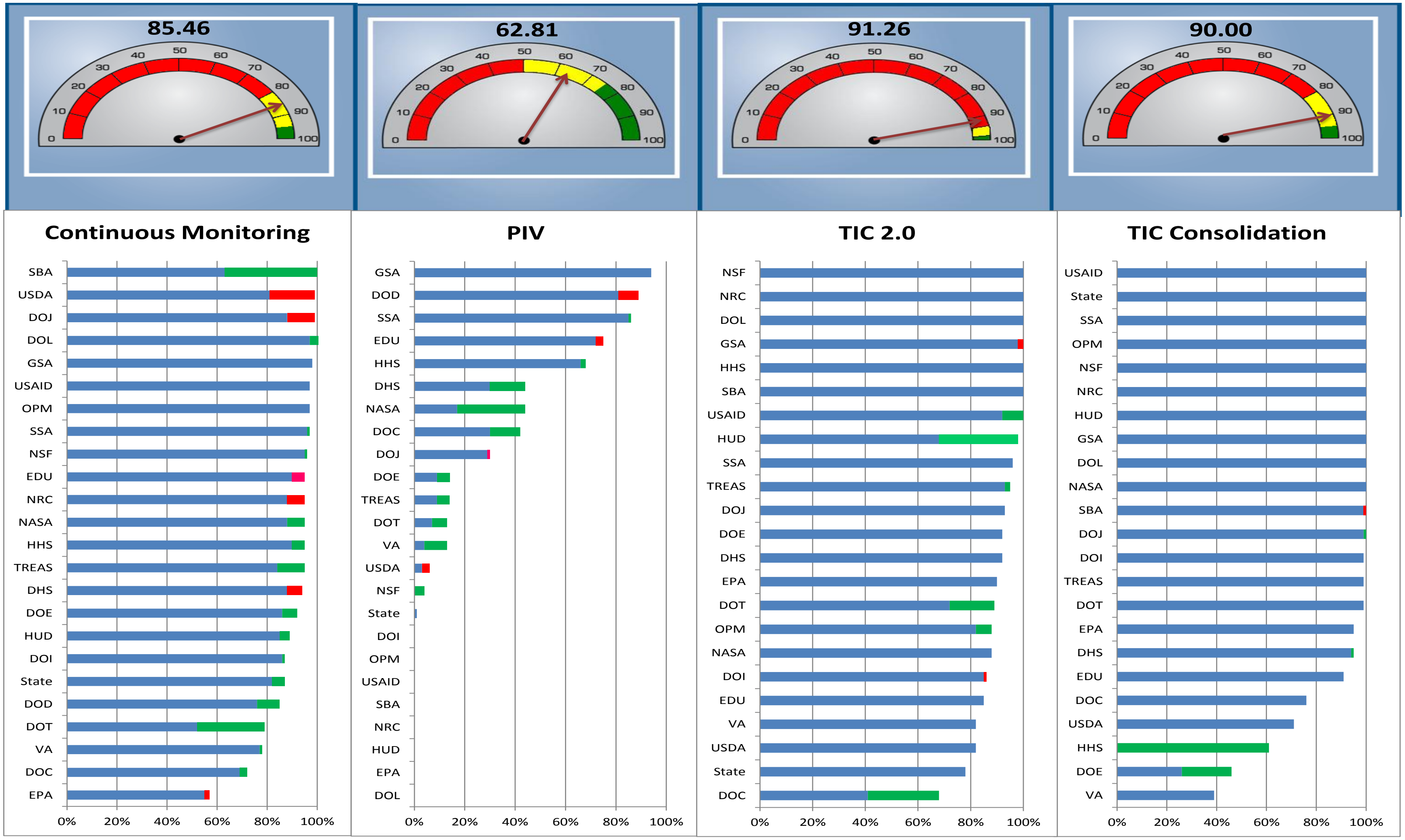
🟩🟩🟩🟩 FY14Q2 => Performance Plan/Goal

→ Better

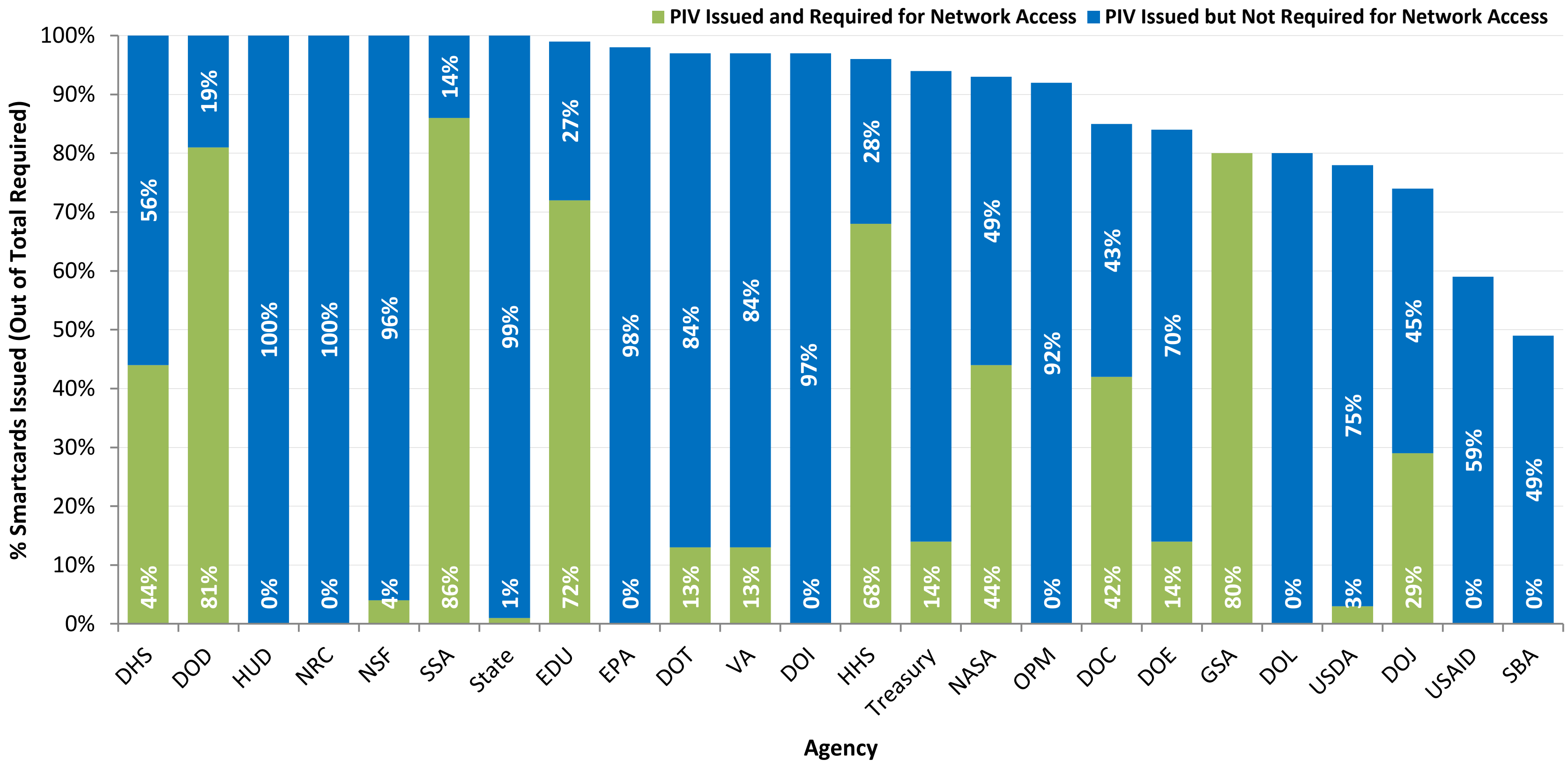
Federal department and agency performance for FY2013 Q4 – FY2014 Q2

The chart below shows each agency's increase (green) or decrease (red) from FY2013 Q4 to FY2014 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.

🟩 FY14Q2 Increase 🟥 FY14Q2 decrease

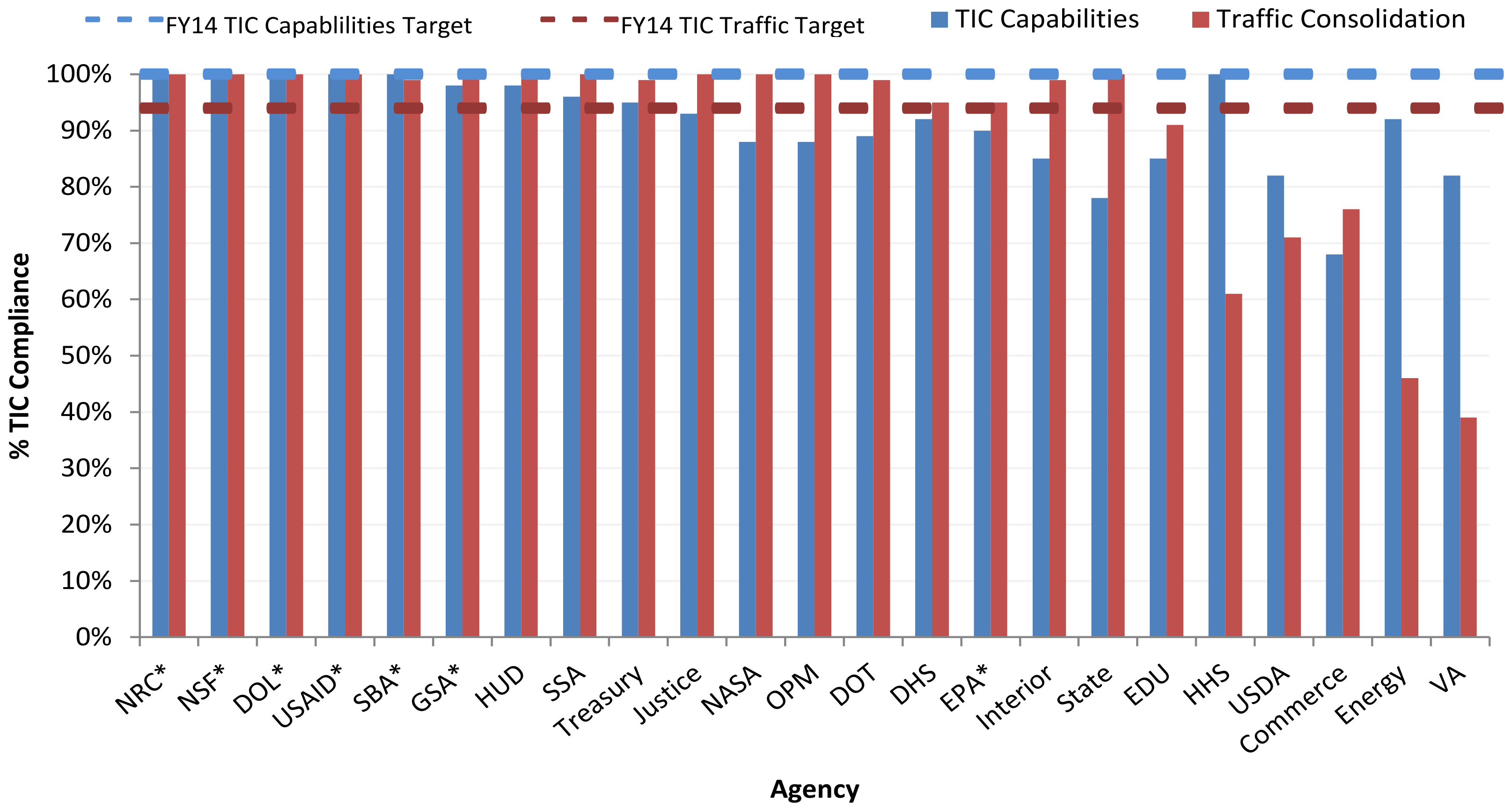


Federal department and agency performance towards Strong Authentication with HSPD-12 Cards as of Q2 FY2014
The chart below shows the percentage of agency employees with HSPD-12 cards, and the percentage that are required to use their cards to authenticate for network access.



PIV Cards Issued as of December 1, 2013: 5,424,900 (96%)
Percentage of accounts requiring use of PIV cards for network logon: 63%
PIV card issuance data from December 2013. PIV card usage data percentages from April 2014
GSA reported 94% usage and 80% 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 Q2 FY2014.



TIC Capabilities represent TIC 2.0 * Agency uses MTIPS provider
TIC Capabilities: Agency FY14 target is 100% ; Government-wide status is 91% (increased 4% from FY13 Q4 to FY14 Q2)
TIC Consolidation: Agency FY14 target is 95%; Government-wide status is 90% (increased 4% from FY13 Q4 to FY14 Q2)

Key Indicators and Metrics

Agency performance uses the FY2014 FISMA metrics and targets, highlighted in Table 2: FY2014 FISMA Metrics.

Administration Performance Area	Annual FISMA Metric Section[11]	Performance Metric	Target Level
Continuous[12] 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.	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	4.1	% 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	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	75%
TIC Consolidation - CNCI[13] #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC[14]).	95%
TIC Capabilities - CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	100%

Table 2: FY2014 FISMA Metrics

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

[12] 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.

[13] Comprehensive National Cybersecurity Initiative (CNCI)

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