

**Strategic Objective: Seek innovative approaches to improve cyber capability against growing threats.**

**OVERVIEW:**

To counter the growing threat in Cyberspace, the DoD is building a Cyber Mission Force (CMF) to increase its capability and capacity to defend priority DoD networks and support joint warfighting requirements. The DoD supports the cyber mission by recruiting and hiring qualified, clearable cybersecurity personnel able to meet target fill rates within the Military Intelligence Program (MIP) and Information Systems Security Program (ISSP).

Threats to the DoD's networks, national critical infrastructure, and U.S. companies and interests continue to evolve, so it is vital to adequately organize, train, and equip the Cyber Mission Force to counter the threat. The Department continues to support the maturation of United States Cyber Command as an operational command to fulfill the DoD's three cyber missions:

1. Defend DoD networks and systems.
2. Defend the United States against cyberspace attacks that have potential to result in significant consequences.
3. Provide full-spectrum cyber options to support contingency plans and military operations.

To fulfill these missions, the DoD works closely with other U.S. Departments and agencies to support investigations of cyber-attacks, and protection of national critical infrastructure. To ensure the DoD can execute these missions, the DoD invests in the following priorities:

- Building the Cyber Mission Force: The Services continue to present personnel to create 133 fully operational teams by the end of FY 2018.
- Training the Cyber Mission Force: The Department is investing in innovative approaches to provide a virtual environment for cyber personnel to consistently train and mission rehearse across a wide range of threat environments.
- Equipping the Cyber Mission Force: The DoD continues to invest in diverse tools, platforms, and infrastructure to be able to conduct all three of its core missions.

## Performance Indicators:

DoD STRATEGIC GOAL #4: Achieve Dominant Capabilities through Innovation and Technical Excellence			
Performance Goals	Performance Measure Indicators	Prior Year Results	FY15 Results
<b>Strategic Objective (SO) 4.2: Seek innovative approaches to improve cyber capability against growing treats.</b>			
PG 4.2.1: By FY 2016, the DoD will include in all new contracts, and as necessary modify contracts associated with critical programs and technology, the DFARS clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (USD (AT&L))	% of all new contracts plus critical programs and technology contracts that include DFARS clause 252.204-4102.	FY10-14 Actual: N/A  New measure - ASP FY2015-2018	FY15 Target: 75 <b>FY15 Result: 75</b>
PG 4.2.2: Build the Military Intelligence Program portion of the Cyber Mission Force (CMF) to improve cyber capability and defend against growing threats. (USD (I))	Fill rate of Military Intelligence Program (MIP) and Information Systems Security Program (ISSP) billets of CMF.	FY10-14 Actual: N/A  New measure - ASP FY2015-2018	FOUO See note on page 21
<p><b>Cross Agency Priority Goal (CAP) - Cybersecurity:</b> Improve awareness of security practices, vulnerabilities, and threats to the operating environment, by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity.</p> <p>Department of Defense engages with the CAP Goal for Cybersecurity initiative. This CAP Goal progress can be located at <a href="http://www.performance.gov">www.performance.gov</a>.</p> <p>The DoD Chief Information Officer (CIO) supports the CAP Cybersecurity Goal and is implementing the DoD Cybersecurity Campaign, Cybersecurity Discipline Implementation Plan, and DoD Cybersecurity Scorecard to rapidly improve cybersecurity posture. These complementary initiatives address the focus areas of the CAP cybersecurity goal, and the DoD Cybersecurity Scorecard includes a list of DoD's prioritized cybersecurity concerns that are reported monthly to the Secretary of Defense.</p> <p>The DCIO for Cybersecurity (CS) is leading and coordinating efforts to limit access to only authorized users and accelerating the implementation of technologies and processes that reduce risk to DoD. Specifically, DoD CIO issued a memorandum and United States Cyber Command issued orders mandating: (1) Immediate review of all privileged user accounts, to include in-person validation and disabling any accounts that are not valid and required, and (2) Accelerated implementation and reporting of DoD public key infrastructure system administrator and privileged user authentication. The Cybersecurity Discipline Implementation Plan also supports the CAP goal objectives with Lines of Effort focused on: Strong Authentication, Device Hardening, Reduce Attack Surface, and Alignment to Computer Network Defense Service Providers.</p>			

*Department of Defense's Data Completeness and Reliability Statement—Fiscal Year 2015 Annual Performance Report*  
Each Goal Owner has attested the performance results and narrative information included in this report is complete, accurate, and reliable; and that data validation and verification procedures are documented and available upon request.

## Measuring our Progress

### FY 2015 APR Progress Update, DFARS Clause 252.204-7012

For FY 2015, the Under Secretary of Defense for Acquisition, Technology and Logistics established a Clause Compliance scorecard to track the inclusion of DFARS Clause 252.204-7012 in all contracts awarded in 1Q FY14 and beyond. The Director, Defense Procurement and

Acquisition Policy (DPAP) publishes the scorecard on a quarterly basis and posts the results to DPAP's Contract Scorecards website

([http://www.acq.osd.mil/dpap/pdi/eb/monthly\\_contract\\_distribution\\_metrics.html](http://www.acq.osd.mil/dpap/pdi/eb/monthly_contract_distribution_metrics.html)) as well as distributes them electronically.

**FY 2015 APR Progress Update, Intelligence Portion of Cyber Mission Force:**

Available upon request