Agency Priority Goal Action Plan

Strengthen Department of Energy (DOE) Cybersecurity

Goal Leader:

Rocky Campione, Chief Information Officer, DOE

Theme(s): Energy

Performance.gov

Fiscal Year 2019, Quarter 4

Overview

Goal Statement

- Strengthen DOE enterprise-wide cybersecurity to protect critical IT infrastructure and ensure continuity of enterprise mission essential functions. By September 30, 2019, DOE will:
  - Expand Departmental enterprise cybersecurity visibility to 90% by deploying sensors and integrating network security data into the iJC3.
  - Reach 100% participation from DOE sites in the scoping, deployment and implementation of enterprise CDM tools to provide scalable, risk-based, cost-effective cybersecurity solutions.
  - Update DOE's Cybersecurity Risk Management Framework for use across Departmental elements and establish standardized enterprise IT cybersecurity requirements.
  - Enhance enterprise-wide cybersecurity governance of project management and architecture to standardize approaches, align with mission essential functions, and reduce technical risks.

Overview

Challenge

- Identifying, managing, and mitigating the increasingly sophisticated and frequent cyber threats occurring on a growing attack surface.
- Centralizing and standardizing tools and requirements across the enterprise with a diverse set of missions, resources, and capabilities.

Opportunity

- Expand the use of modern commercial technologies that are effective, economical, and secure; reduce the impact of cybersecurity risks by safeguarding IT systems, sensitive data, and networks; leverage common solutions and innovative practices to improve efficiency and increase security.

Goal Structure & Strategies

Strategies: To effectively strengthen its network cybersecurity, DOE will coordinate with senior agency leadership to advance agency-level processes and apply the following strategies:

DOE Cybersecurity Strategy and Strategic Plan	Continuous Diagnostics and Mitigation (CDM)	Cooperative Protection Program (CPP)	Big Data Platform (BDP)	Enterprise Risk Management
The DOE Cybersecurity Strategy (approved June 2018) includes implementation of Continuous Diagnostics and Mitigation (CDM) tools, enhancing DOE's Integrated Joint Cybersecurity Coordination Center (iJC3) to ensure increased enterprise visibility of the cyber attack surface, and implementing a cyber risk management framework to prioritize investments and improve our responses to rapidly evolving threats.	In coordination with DHS, DOE will fully implement CDM tools across the enterprise to provide: • A centralized enterprise inventory of hardware and software • Readily accessible data through the DOE dashboard to produce customized reports to inform and prioritize cyber risk assessments across the Department • Integration with the Big Data Platform.	In order to increase cybersecurity visibility at the headquarters level, the iJC3 is coordinating with DOE program offices, sites, and labs to deploy updated network sensors to capture detailed information on network traffic to feed into the Big Data Platform.	A cloud based solution that was developed for the Defense Information Systems Agency (DISA) and implemented by U.S. Cyber Command (USCYBERCOM), the National Security Agency (NSA) and multiple Department of Defense (DoD) mission partners, BDP will aggregate data from across the DOE enterprise and provide: • Timely access to critical data • Hunting across historic data utilizing advanced analytics • Single point of access for cyber tools • Automated process support	The near real-time data from CDM and BDP will enable leadership to make more informed risk-based decisions. To support this effort, the DOE will implement an updated IT Risk Management Framework to standardize the approach to identifying, assessing, and managing risk.

Summary of Progress – Final

Progress Summary

- Improve Cybersecurity Visibility: The Department has expanded enterprise cybersecurity visibility by maintaining CPP sensors and integrating the data produced by these sensors into the Department's Integrated Joint Cybersecurity Coordination Center (iJC3).
- Continuous Diagnostics and Mitigation (CDM): 100% of DOE sites are participating in the CDM program. The Department completed analysis to determine gaps and availability of site cybersecurity asset and vulnerability management tools. Upon completion of the analysis, the Department began to integrate data from existing tools and prepare for procurement and implementation of new tools.
- Enterprise Risk Management: The Department issued DOE Order 205.1C, Cybersecurity Program on May 15, 2019. Policy implementation is underway and is focused on transitioning from a posture of risk acceptance to one of risk management across Departmental stakeholders. The Order requires annual Cybersecurity Program plans, annual Risk Assessments with quarterly updates, and Cybersecurity Enterprise Risk Management to include Supply Chain Risk Management. The OCIO has implemented an enterprise Cybersecurity Risk Management Program (eCRM) to develop and deploy a blended risk methodology that combines qualitative and quantitative risk assessment and evaluation methods to support departmental eCRM program execution.
- Enhance Corporate governance: The Enterprise Architecture Governance Board was established in November 2018 and continues to serve as the primary means to enhance the Department's Enterprise Architecture Framework and mature the information management process.

Statement of Goal Achievement and Next Steps

Goal Statement

- Strengthen DOE enterprise-wide cybersecurity to protect critical IT infrastructure and ensure continuity of enterprise mission essential functions. By September 30, 2019, DOE will:
  - Expand Departmental enterprise cybersecurity visibility to 90% by deploying sensors and integrating network security data into the iJC3. **Met**
  - Reach 100% participation from DOE sites in the scoping and preparing for deployment and implementation of enterprise CDM tools to provide scalable, risk-based, cost-effective cybersecurity solutions. **Met**
  - Update DOE's Cybersecurity Risk Management Framework for use across Departmental elements and establish standardized enterprise IT cybersecurity requirements. **Met**
  - Enhance enterprise-wide cybersecurity governance of project management and architecture to standardize approaches, align with mission essential functions, and reduce technical risks. **Met**

APG Status: **Achieved**

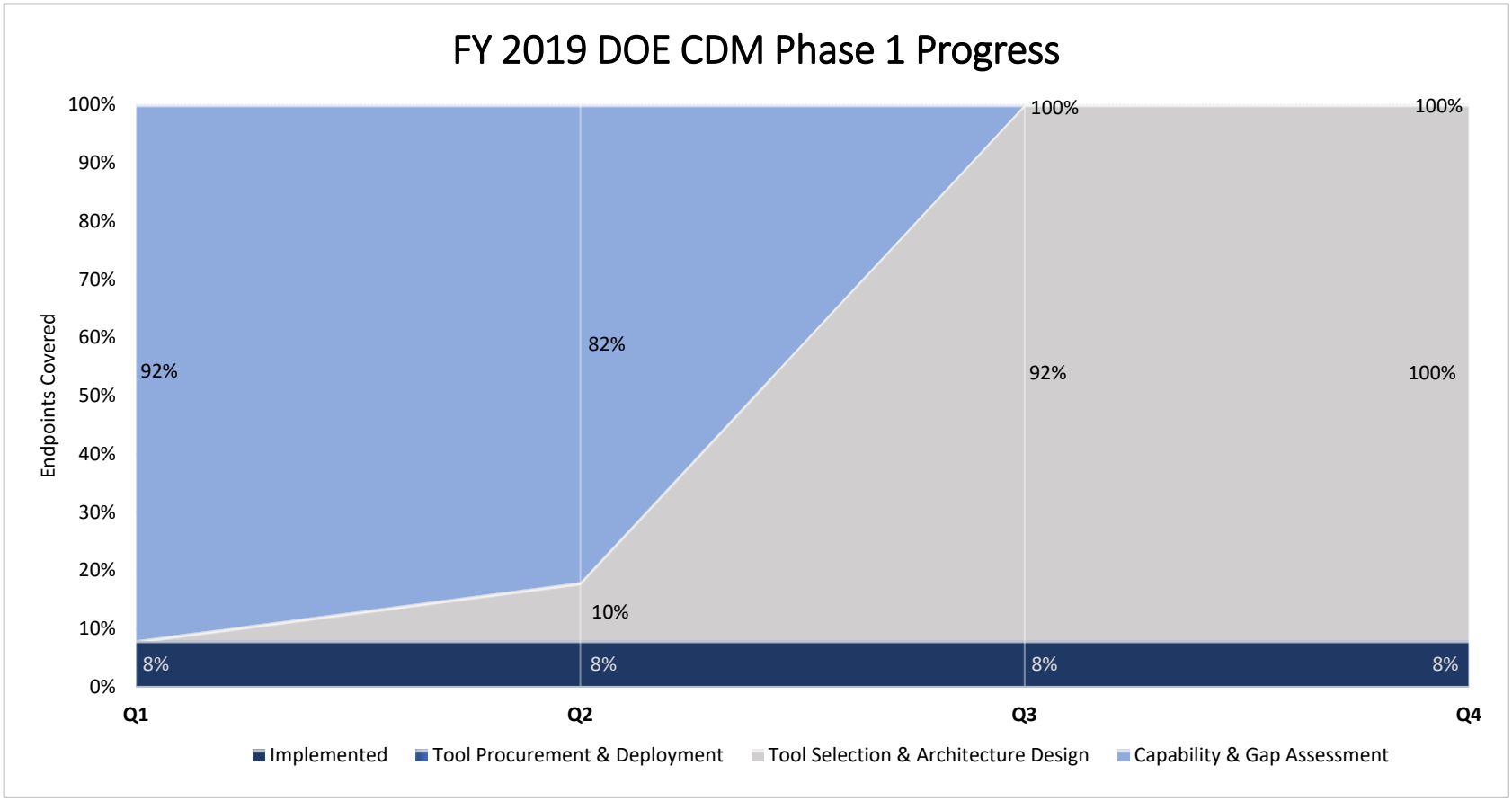
Next Steps:

- Does DOE have an FY 2020-2021 APG in this topic area? **Yes**

Key Milestones

Key Milestone	Milestone Due Date	Milestone Status
Improve Cybersecurity Visibility		
BDP Development, Staging and Production Environments Established	FY18 Q2	Completed
BDP ATO Completed	FY18 Q4	Completed
Cooperative Protection Program (CPP) – Network Sensor Enhancements deployed to enterprise	FY19 Q2	Completed
iJC3 - Big Data Platform (BDP) Initial Operational Capability Implemented	FY19 Q2	Completed
Continuous Diagnostics and Mitigation (CDM)		
Complete DOE Continuous Diagnostics and Mitigation (CDM) Phase 1 Gap Fill Request for Service (RFS) 10 capability and gap assessment and tool selection/architecture design	Original Milestone: Due Date: FY 19 Q3 Revised Due Date: FY20 Q2	Revised Milestone Completion Date
Enterprise Risk Management		
Update DOE 205.1B – Department of Energy Cybersecurity Program	FY19 Q3	Completed
Enhance Corporate Governance		
Establish a phased Enterprise Architecture strategy and initial roadmap that facilitates development and rationalization of the DOE security architecture in support of the Integrated Joint Cybersecurity Coordination Center (iJC3) encompassing CDM, BDP, and CPP	FY19 Q2	Completed

Key Indicators – CDM Timeline



This graph is a representation of the percentage of completion for each of the DOE CDM Phases

- **Implemented:** phase denotes a % of DOE endpoints that have fully implemented the CDM tools
- **Tool Procurement & Deployment:** phase captures the % of DOE complex that have selected tools and are now in the procurement and/or tool deployment phase (Note: progress for FY2019 is 0%)
- **Tool Selection & Architecture Design:** phase represents the % of DOE endpoints that are currently in the phase of evaluating and selecting tools to be implemented
- **Capability & Gap Assessment:** phase of the graph is a representation of the % of DOE complex that is still in the capability & gap assessment phase, and have not yet started selecting tools

Note: reporting reflected as of end-of-quarter

Additional Information

Contributing Programs

Organizations:

- National Nuclear Security Administration (NNSA)

  Collaborate in cybersecurity governance and management, coordinate cybersecurity monitoring, reporting, and response.

- Departmental Element Security/Network Operations Centers (SOCs/NOCs)

  Coordinate incident management and reporting.

- Departmental Element CIOs/Chief Information Security Officers (CISOs)

  Collaborate cybersecurity governance and management, coordinate cybersecurity monitoring, reporting, and response.

- DHS NCCIC and Federal Network Resilience (FNR)

  DHS's goal to strengthen Federal cybersecurity and its supporting cybersecurity programs, services, and tools help equip DOE for their cybersecurity and risk management activities.

Additional Information

Stakeholder / Congressional Consultations

- Energy Infrastructure

  Lend technical expertise and collect insights through coordination with DOE Cybersecurity, Energy Security, and Emergency Response (CESER)

- Office of Management and Budget (OMB)

  Leverage OMB guidance and director in formulation, implementation, and monitoring of DOE cybersecurity and risk management activities

- Congress

  Assess Congressional legislation in formulation, implementation, and monitoring of DOE cybersecurity and risk management activities

- Government Accountability Office (GAO)

  Consider GAO reporting on DOE cybersecurity matters in formulation, implementation, and monitoring of DOE cybersecurity and risk management activities

- Agency Inspectors General (IGs)

  Consider GAO reporting on cybersecurity matters in formulation, implementation, and monitoring of DOE cybersecurity and risk management activities