Agency Priority Goal Action Plan

Department of Energy (DOE) Enterprise Cybersecurity

Goal Leader(s):

Rocky Campione, Chief Information Officer
Greg Sisson, Acting Deputy Chief Information Officer for Cybersecurity, and Chief Information Security Officer

Overview

Goal Statement

Assess all Department high value assets/systems and implement mitigation strategies consistent with the risk to national security interests and the success of the DOE mission essential functions. By September 30, 2021 DOE will develop and deploy enhanced assessments, updated risk management strategies, continuous monitoring, and cybersecurity mitigations for 100% of the Department's High Value Assets (HVA).

Challenge

Protect the Department's most critical systems and information

Opportunity

Evolve the management of HVAs to gain more operational visibility and provide increased risk management awareness

Leadership & Implementation Team

Oversight and Project Management

Chief Information Officer (CIO), Chief Information Security Officer (CISO)

Privacy

Senior Lead:
- Chief Privacy Officer / Senior Agency Official for Privacy

Team Leads:
- Supervisory Policy Information Specialist

Agency Partners:
- Office of Management and Budget (OMB)

Cyber

Senior Lead:
- Director of Cybersecurity Operations, Office of the Chief Information Officer

Team Leads:
- HVA Program Manager
- Integrated Joint Cybersecurity Coordination Center (iJC3)

Agency Partners:
- Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA) HVA Project Management Office (PMO)

Data

Senior Lead:
- Chief Data Officer

Team Leads / Internal Partners:
- Program Offices and Sites

Assessment(s)

Senior Lead:
- Enterprise Assessments (EA)
- Office of the Chief Information Officer, Cybersecurity
- DOE Inspector General

Team Leads:
- HVA System Owners

Agency Partners:
- Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA) HVA PMO

Fiscal

Senior Lead:
- Chief Financial Officer (CFO)

Team Leads:
- Senior Technical Advisor / Director, Federal Information Technology Acquisition Reform Act (FITARA)

Agency Partners:
- Office of Management and Budget (OMB)

Goal Structure & Strategies

1. Operational Visibility

A. Maintaining HVA Inventory

- Revalidate DOE's HVA inventory in alignment with OMB definition and DHS/CISA criteria

B. Prioritization of HVAs

- Implement HVA prioritization methodology to focus maximum effort on top HVAs

C. Continual Situational Awareness

- Establish HVA Dashboard to visualize key metrics

2. Risk Management

A. Continuous Monitoring

- Implement all available assessment services and methods
- Leverage Continuous Diagnostics and Mitigation (CDM) capability when available

B. Plan of Action and Milestone (POA&M) Management

- Monitor progress of DOE's POA&Ms utilizing Enterprise Cyber Governance System (ECGS)

C. Remediation Support

- Assist HVA owners to remediate vulnerabilities and findings

Goal Structure & Strategies

Operational Visibility

	Percent Complete (%)
1.A. Maintaining HVA Inventory – Revalidation Progress*	100
1.B. Prioritization of HVAs – Prioritization Progress*	100
1.C. Continual Situational Awareness - HVA Dashboard Development	100

Risk Management

	Percent Complete (%)
2.A. Continuous Monitoring – Assessments Completed*	47
2.B. POA&M Management - POA&Ms not Delayed	TBD

*Percentages based on dynamic count of HVAs – 19 as of 9/30/2020

Summary of Progress – FY 20 Q1

- Conducted two monthly DOE HVA Stakeholder update meetings
- Completed initial Enterprise Cyber Governance System (ECGS) gap analysis for HVA system information and found only some HVAs have current POA&Ms documented
- Developed and distributed a revised HVA data call, which added ten new questions, removed three, expanded three, and adjusted two
- Participated in an Inter-Agency Working Group for revision of DHS/CISA Analytical Hierarchical Process (AHP) for prioritizing HVAs
- DHS/CISA completed one HVA assessment and provided two recommendations
- DOE OCIO released the Draft FY20 FISMA Inventory Methodology, which describes requirements for identification of HVAs

Goal Status: On target

Summary of Progress – FY 20 Q2

- Conducted one monthly DOE HVA Stakeholder update meeting
- Conducted quarterly Binding Operational Directive (BOD) 18-02 data call, submitted results for 22 HVAs to DHS/CISA via Cyberscope
- Continued participation in an Inter-Agency Working Group for revision of DHS/CISA Analytical Hierarchical Process (AHP) for prioritizing HVAs
- DHS/CISA conducted one HVA assessment February 10-11, 2020
- DOE/EA conducted assessments on four HVA

Goal Status: On target

Summary of Progress – FY 20 Q3

- Conducted two monthly DOE HVA Stakeholder update meetings
- Began participation in an Inter-Agency HVA Program Gap Analysis Working Group
- DOE/EA conducted assessments on two HVAs with no significant recommendations
- DOE/OCIO sponsored a vendor to conduct a crowdsourced assessment on one HVA; recommendations are pending upon release of final report
- Published the DOE HVA Program Plan to describe how the Program operates
- Established the HVA Executive Dashboard to visualize key metrics and provide continual situational awareness to stakeholders

Goal Status: On target

Summary of Progress – FY 20 Q4

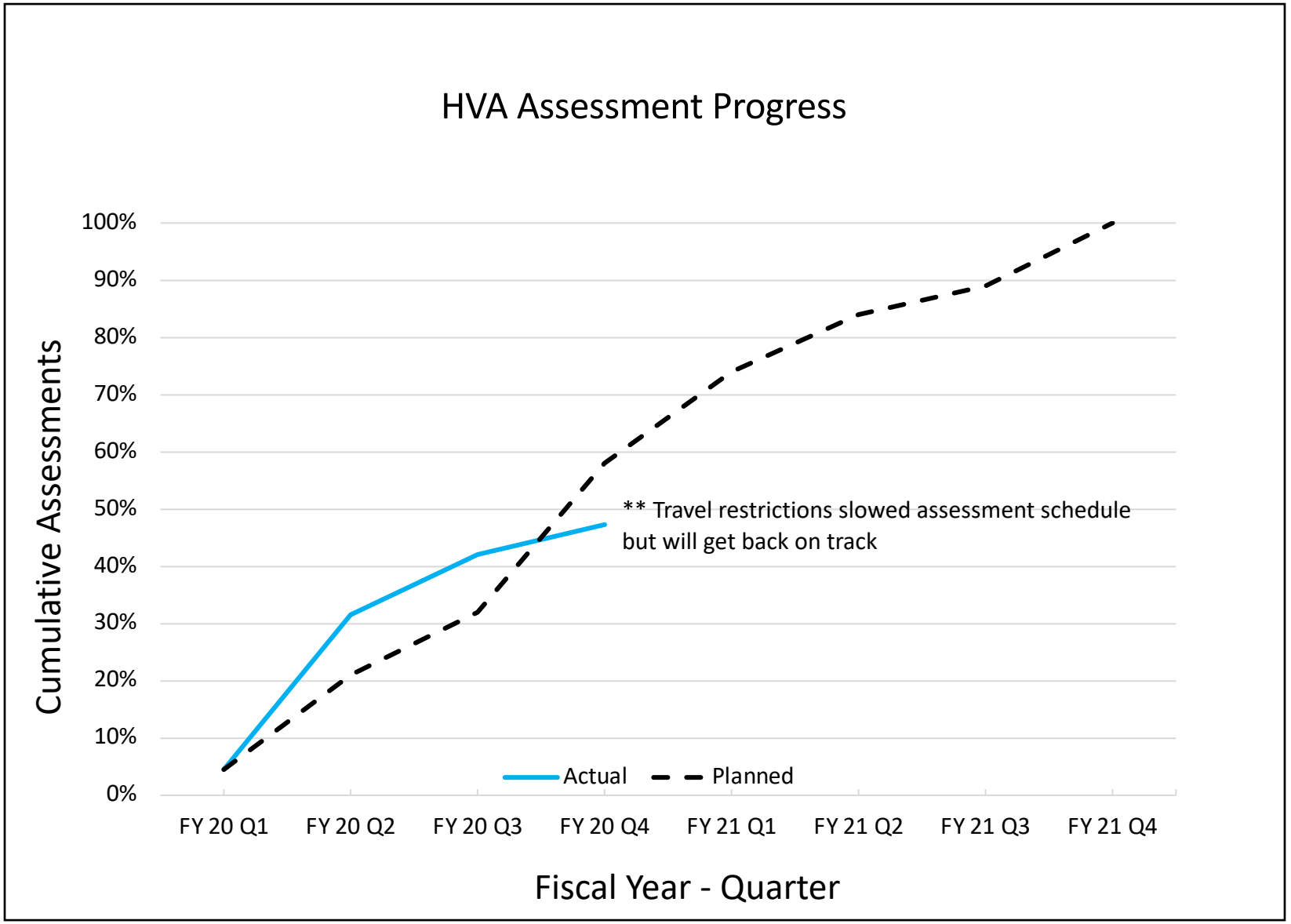
- Conducted one monthly DOE HVA Stakeholder update meeting
- Completed a crowdsourced assessment on one HVA via an independent third party
- Implemented enhancements to the HVA Executive Dashboard with host and domain names
- Continued interagency collaboration through the Federal CISO Council HVA Subcommittee Meeting
- Tentatively scheduled three Tier-1 HVAs for DHS CISA Validated Architecture Design Review (VADR) assessments
- Submitted the BOD 18-02 HVA data call to DHS CISA via CyberScope

Goal Status: On target

Key Milestones

Milestone Summary			
Key Milestone	**Milestone Due Date**	**Milestone Status**	**Comments**
DHS/CISA HVA Data Call conducted every quarter	FY20 Q1	Completed	HVA data call structure/procedures revised in FY20 Q1. Subsequent data calls to be released quarterly. "Conducted" indicates full range of data call lifecycle activities. Quarterly data call validates existing HVAs and presents opportunity to add new HVAs to meet evolving selection criteria.
HVA Inventory Revalidated	FY20 Q2	Completed	Data call expansion and tightened criteria will lead to a revalidated inventory
HVA Prioritization Methodology Implemented	FY20 Q3	Completed	Adapted DHS prioritization methodology guidance
HVA Dashboard Established	FY20 Q3	Completed	Collaborated with the DOE Integrated Joint Cybersecurity Coordination Center (iJC3)
Updated Risk Management Strategies Develop and Deployed	FY20 Q4	Completed early in Q3	Risk Management Methodology Amplification Guidance document distributed
Continuous Monitoring Developed and Deployed	FY21 Q1	In Progress	Includes Quarterly Data Call activity, Assessments, CDM, and HVA Executive Dashboard enhancements
Enhanced Assessments Developed and Deployed	FY21 Q2	In Progress	Engagement with DOE independent third-party assessment team
Cybersecurity Mitigations Developed and Deployed	FY21 Q3	TBD	Includes POA&M tracking and remediation support
100% of HVA Critical and High POA&Ms mitigated without delay	FY21 Q4	TBD	
100% of the Department's HVAs Assessed	FY21 Q4	TBD	

Key Indicators



Data Accuracy and Reliability

HVA Data Call: Issued quarterly across the Department for HVA owners to provide self-reported information and data on status of IT/OT systems

Enterprise Cyber Governance System (ECGS): The system of record and data repository for IT systems that tracks Plan of Action and Milestones (POA&M) record updates and changes, input by the HVA owners and validated by the HVA Program Office

Inspector General (IG) or GAO Audits: Independent assessments usually conducted at the site level

Enterprise Cyber Assessments (EA-60): Independent assessments usually conducted at the site level

DHS/CISA Assessments: Independent assessments conducted on Tier-1 HVAs

Additional Information

Organizations:

- OMB sets the overall direction for HVA program accomplishments and management
- DHS/CISA HVA PMO provides guidance to DOE on performing assessments
- Integrated Joint Cybersecurity Coordination Center (iJC3) provides metrics on incidents and vulnerabilities affecting DOE IT systems, data, and operations

President's Management Agenda:

- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, provides guidance on the enhancement of HVA programs including expectations for enterprise HVA governance, HVA designation improvement, HVA data-driven prioritization, increasing HVA trustworthiness, HVA privacy protections, and defining HVA reporting, assessment, and remediation requirements

Program Activities/Regulations:

- DOE HVA Stakeholder Monthly Meeting – Stakeholders receive guidance, exchange lessons learned, and collaborate to meet requirements

Policies:

- DHS Binding Operational Directive (BOD) 18-02, Securing High Value Assets – requires all Federal agencies to prioritize the security of their most critical and high impact systems
- DOE Order 205.1C, Department of Energy Cyber Security Program – requires Department Elements to identify, report, and manage HVA in accordance with OMB requirements, submit monthly POA&M updates, and conduct HVA inventory management

Other Federal Activities:

- N/A