



Homeland Security

FY 2020 - 2022 Annual Performance Report

Appendix C: DHS Agency Evaluation Plan

With honor and integrity, we will safeguard the American people, our homeland, and our values.

About this Report

The U.S. Department of Homeland Security Annual Performance Report (APR) for Fiscal Years (FY) 2020-2022 presents the Department's performance measure results and FY 2021 and FY 2022 targets. It also summarizes information on key initiatives in the DHS Performance Management Framework related to the Strategic Review, our FY 2020 results for the Department's Agency Priority Goals (APG), and also includes the Human Capital Operating Plan. The report is consolidated to incorporate our annual performance plan and annual performance report.

For FY 2020, the Department's Performance and Accountability Reports consist of the following three reports:

- DHS Agency Financial Report | Publication date: November 16, 2020
- DHS Annual Performance Report | Publication with the DHS Budget
- DHS Report to our Citizens (Summary of Performance and Financial Information) | Publication date: March 29, 2021

When published, all three reports will be located on our public website at: <http://www.dhs.gov/performance-accountability>.



Contact Information

For more information, contact:
Department of Homeland Security
Office of the Chief Financial Officer
Office of Program Analysis and Evaluation
245 Murray Lane, SW
Mailstop 200
Washington, DC 20528

Table of Contents

Department of Homeland Security: FY 2022 Annual Evaluation Plan	2
Contact.....	2
Program: CISA High Value Asset (HVA) Program	2
<i>Lead Organization</i>	<i>2</i>
<i>Program Description</i>	<i>2</i>
<i>Purpose and Scope</i>	<i>3</i>
<i>Resources</i>	<i>3</i>
<i>Questions.....</i>	<i>3</i>
<i>Information Needed</i>	<i>3</i>
<i>Design and Methods</i>	<i>4</i>
<i>Anticipated Challenges and Limitations.....</i>	<i>4</i>
<i>Dissemination and Use.....</i>	<i>4</i>
Program: CISA Exercises.....	5
<i>Lead Organization</i>	<i>5</i>
<i>Program Description</i>	<i>5</i>
<i>Purpose and Scope</i>	<i>5</i>
<i>Resources</i>	<i>6</i>
<i>Questions.....</i>	<i>6</i>
<i>Information Needed</i>	<i>6</i>
<i>Design and Methods</i>	<i>6</i>
<i>Anticipated Challenges and Limitations.....</i>	<i>7</i>
<i>Dissemination and Use.....</i>	<i>7</i>

Department of Homeland Security: FY 2022 Annual Evaluation Plan

The Foundations for Evidence-Based Policymaking Act of 2018 (“Evidence Act”) requires that the DHS Evaluation Officer coordinate and issue an Annual Evaluation Plan concurrent with the Annual Performance Plan, describing “significant” evaluations and related information collections and acquisitions planned for the subsequent fiscal year.

The DHS Annual Evaluation Plan consists of a subset of the Department’s evaluation work for the subsequent fiscal year. These evaluations, designated as significant, are shared with the American public and receive additional resources to ensure successful completion. The list below highlights the criteria DHS considers when making the significant evaluation designation:

- Supports DHS Learning Agenda
- Responds to mandate
- Aligns with leadership priorities
- Has potential for agency-wide impact or engagement
- Has potential for high financial impact
- Has potential for high stakeholder impact

The FY22 Annual Evaluation Plan includes two significant evaluations that are described below:

1. Cybersecurity and Infrastructure Security Administration (CISA) High Value Asset (HVA) Program Evaluation; and
2. CISA Exercises Evaluation.

Contact

Mike Stough, DHS Evaluation Officer

Program: CISA High Value Asset (HVA) Program

Lead Organization

CISA Program Analysis and Evaluation (PA&E)

Program Description

Due to rapidly emerging threats and capacity gaps, federal departments and agencies require targeted effort to identify risks to the most sensitive government IT systems and data – high value assets – and support in protecting them. The HVA program office conducts tailored assessments for department and agency HVAs to identify risks, crafts recommendations for mitigating them, and provides targeted support to assist federal entities in their remediation efforts. The program aims to increase overall federal enterprise security and resilience, prevent data compromise and loss, and reduce disruption of critical services and operations involving HVAs.

Purpose and Scope

The primary purpose of the evaluation is to compare actual program implementation against the intended approach and measure the benefits agencies experience from participating in the program, including those benefits that were unintended. The evaluation will measure the level of consistency in processes and procedures across assessments as well as the key barriers that prevent agencies from completing mitigation and remediation actions. The results will inform improvements to product and service delivery and provide insights into the factors that are most important to ensure departments and agencies take timely action to mitigate risks.

The evaluation will focus on the assessment processes and procedures; the dissemination of assessment reports, identified risks, and recommended remediation actions; oversight of department and agency remediation efforts and compliance with Binding Operational Directive (BOD) requirements during the time period of fiscal years 2018-2021.

Resources

The evaluation will be conducted externally through a contract mechanism that CISA plans to solicit, award, and execute beginning in FY21 for evaluation activities. CISA currently estimates a 12-month period of performance in FY22.

Questions

The evaluation will address the following key questions:

1. What is the variation in execution of assessments, compared with the standards in the defined assessment process guide?
2. Why is variation occurring?
3. Are CISA and agency stakeholders disseminating and briefing results and recommended corrective actions at the right levels, and do those efforts trigger corrective action?
4. What are the benefits and unintended consequences for program participants of identifying risks and implementing recommendations?
5. What are the barriers that program participants face in implementing recommendations and their current efforts to overcome them?

Information Needed

The evaluation will require the following information for which data are available: number of HVA assessments conducted; average time for assessment completion; qualitative data on assessment execution compared with defined process guide for assessments; and percentage and nature of timely remediation actions.

The evaluation will require the following information for which new data collection is necessary: level of customer satisfaction with assessment process and results; number of dissemination and briefing activities conducted, disaggregated by type; benefits and unintended consequences for

program participants of identifying risks and implementing recommendations; and identified barriers to timely remediation actions

Design and Methods

This is a process/ implementation evaluation with a non-experimental (observational) design.

Primary data sources include CISA HVA program staff; agency Chief Information Officers (CIO) and Chief Information Security Officers (CISO); Agency CIO and CISO staff (agency HVA program managers); HVA inter-agency working group members; and CISA HVA assessors. Secondary data sources include HVA program administrative data on number of assessments and status of remediation actions; and BOD compliance data.

Surveys will be fielded with all agency HVA points of contact. Stakeholder focus groups and key informant interviews will be conducted with a CISA HVA program staff and assessors, agency CIOs and CISOs, agency HVA program managers, and HVA interagency working group members.

Descriptive statistical analysis will be used for quantitative survey data and program administrative data. Qualitative analysis, including cross-site analysis and theme identification, will be used for program administrative data and qualitative data collected through surveys, interviews and focus groups.

Anticipated Challenges and Limitations

Data on internal agency briefings may be difficult to get. Agencies may be reluctant to share detailed information about the reasons they are unable to implement recommended actions.

Consistent and reliable measurement of assessor competencies and the knowledge level of the technical point of contact for a given assessment may be difficult and could limit available information for use in the evaluation. Lack of adequate representation of key agency characteristics in focus groups and key informant interviews could limit the validity and applicability of findings. Participation in inter-agency HVA working groups may be biased towards agencies with higher capacity and greater interest in the program. Agency reporting against FISMA and BOD requirements may require additional clarification to ensure accuracy and intended information.

Dissemination and Use

The primary user is the CISA HVA program office, which will leverage the results to gain deeper understanding about the factors that affect agencies' ability to implement corrective actions and to determine how to refine assessment processes and agency engagement approaches to meet agencies' needs. The program office will also use the findings about variation in the assessment process to refine the assessment approach and improve assessment data quality. CISA leadership will use the results to understand how to engage with leadership at customer agencies to address escalation issues effectively. The evaluation will inform OMB's understanding of funding and resources needed to better support agencies' mitigation efforts. The federal CISO community will

use the results to better understand and apply lessons learned to the mitigation efforts at their agencies.

There are no limitations on public disclosure anticipated at this time.

Program: CISA Exercises

Lead Organization

CISA PA&E

Program Description

CISA stakeholders (including federal, state, and local government and private sector critical infrastructure owners and operators) are insufficiently prepared to address physical/cybersecurity threats and incidents. They may lack awareness of threats and vulnerabilities. They may possess insufficient subject matter expertise within their organizations. Some may lack key capabilities and/or plans to effectively prevent, protect against, respond to, or mitigate threats and hazards. Or, they may lack relationships with key partners. CISA Exercises leverages the Homeland Security Exercise and Evaluation Program process to design, plan, and execute exercises that engage stakeholders in identifying threats and vulnerabilities; assessing risk-mitigating measures, plans, and capabilities; and connecting with other community partners and relevant resources. CISA Exercises build national preparedness and resilience through the enhancement of individual, organizational, and community awareness, planning, and capabilities.

Purpose and Scope

The purpose of this evaluation is to measure the degree to which CISA Exercises program customers (voluntary participants from federal, state, and local government and private sector critical infrastructure owners and operators) are implementing the recommended corrective actions identified through the exercise process, and, in cases where they are not, to better understand the major factors limiting corrective action implementation. The long-term outcome of increased preparedness and resilience is dependent upon the intermediate-term outcome of customers implementing corrective actions to address planning and capability gaps identified through the exercise process. The results of the evaluation will inform CISA Exercises, other CISA capability-building programs, and CISA at-large about how best to leverage and improve upon its capability-building approaches.

The evaluation will focus on assessing whether exercise customers are taking action on recommended steps to address planning and capability gaps identified in the exercise process and identifying organizational demographic or other factors that affect whether actions are taken. In cases where corrective actions are not implemented, it will investigate the major factors that limit or prevent that, such as how program activities (e.g., planning meetings and exercise discussions) and outputs [e.g., exercise after-action reports (AARs)] are framed, as well as how exercise services are targeted. It will also elucidate factors and barriers to corrective action

implementation. The evaluation will study exercises conducted in the two-year time period of fiscal years 2020 and 2021.

Resources

The evaluation will be conducted externally through a contract mechanism that CISA plans to solicit, award, and execute beginning in FY21 for evaluation activities. CISA currently estimates a 12-month period of performance in FY22.

Questions

The evaluation will address the following key questions:

1. Are customers taking corrective action to address planning/capability gaps identified through the exercise process?
2. What type of corrective actions are most/least frequently implemented?
3. Are there any correlations between customer demographics and actions taken/not taken?
4. If customers are not taking action to address planning/capability gaps identified through the exercise process, what are the facilitators and barriers to corrective action implementation?
5. What steps can be taken, and by whom, to overcome factors limiting corrective action implementation?

Information Needed

The evaluation will require the following information for which data are available: Level of quality, effectiveness, and customer satisfaction with the exercise at the time (or shortly after) the exercise is conducted.

The evaluation will require the following information for which new data collection is necessary: category (type) of corrective actions implemented; and potential facilitators and barriers of enactment of corrective action implementation.

Design and Methods

This is a mixed-methods implementation and outcome evaluation with a non-experimental (observational), single group post-program design.

Primary data sources include customers (including federal, state, and local government and private sector critical infrastructure owners and operators) that have participated in CISA Exercises services in the past 24 months. Secondary data sources include Exercises program administrative data, including planning and exercise artifacts and AARs, which identify planning and capability gaps and corrective actions that are, in part, the subject of follow-up data collection.

Surveys will be fielded with exercise customers, including the CISA Exercises Post-Exercise Survey (immediately post-participation) and the CISA Exercises 6-Month Follow-up Survey data.

Customer focus groups and key informant interviews will also be conducted with exercises customers.

Descriptive statistical analysis will be used for quantitative survey data. Qualitative analysis, including cross-site analysis, theme identification, and development of case study descriptions, will be conducted with program administrative data and qualitative data collected through surveys, interviews and focus groups.

Anticipated Challenges and Limitations

Collecting data from customers on the degree to which corrective actions are being taken, and the factors that may limit a customer's ability to implement corrective actions, presents challenges, including customer interest in or willingness to share this information. The understanding resulting from this evaluation may yield a better appreciation for the challenges customers face, but the program may have limited ability to effect change in customer actions.

Reaching an appropriate response rate on customer satisfaction surveys may be a challenge that limits validity and generalizability of findings. Customers comprise a wide-variety of stakeholder groups and organizational demographics, each with unique capabilities, needs, resources, and circumstances, which may limit the degree to which data received from any specific customer can be generalized to be meaningful or useful beyond that specific customer. Additionally, for a variety of reasons, data obtained through surveys or interviews may be biased toward customers who are more likely to have taken corrective actions as a result of participation in exercises.

Dissemination and Use

CISA Exercises will use the evaluation results to guide and refine future product and service development and delivery, possibly including where to focus future exercises. Other CISA capability-building program offices can potentially use the evaluation results in a similar manner to guide and refine future product and service development and delivery (based on applicability to their program, products, and services). The results may increase CISA program offices' understanding and appreciation of the range of challenges and limitations encountered by this sample of their customers in implementing security improvements recommended by the programs. Additionally, results could identify potential opportunities/growth areas for CISA. CISA leadership can use the evaluation results to better understand the major levers that can be pulled to reduce barriers to security enhancement.

CISA will share the results of the evaluation with other relevant offices within DHS that could benefit from the insights and analysis provided through the evaluation. This could include the National Exercise Division and National Preparedness Assessments Division of the Federal Emergency Management Agency, as well as other exercise programs through the DHS Exercise Coordination Group.

There are no limitations on public disclosure anticipated at this time.



Homeland
Security



Homeland
Security