Guidehouse
Outwit *Complexity*

How to Prepare for Cybersecurity & Infrastructure Security Agency High Value Asset Assessments

The US Government currently has more than 800 unique High Value Asset (HVA) systems, and agencies are required to have qualified assessors perform HVA assessments on their systems every three years. Are you ready?

History of the High Value Asset Program

In 2015, the US Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) created the High Value Asset (HVA) initiative as a component of the Cybersecurity Strategy and Implementation Plan. This was followed by the first set of implementation guidance in December 2016[1] and the first version of the HVA Control Overlay in 2017 (superseded by version 2.0 in January 2021).[2] The HVA Control Overlay, created to provide guidance to federal civilian agencies to protect their HVA systems, is based on National Institute of Standards and Technology 800-53 controls and is currently an optional guidance.

With the creation of the Cybersecurity and Infrastructure Security Agency (CISA) in late 2018, DHS centralized its HVA responsibilities. In 2018, CISA released BOD-18-02[3] which, among other things, required all agencies to:

- Identify agency HVA points of contact.
- Submit a prioritized list of HVAs to CISA.
- Participate in DHS-led assessments.

In 2019, OMB released M-19-034 which, among other things, gave DHS and CISA the responsibility and authority to oversee and require the completion of HVA assessments.

NT1 Assessment Details

The BOD 18-02 requires agencies to identify and designate HVAs, which CISA then designates as either Tier 1 or Non-Tier 1 (NT1), depending on such variables as system complexity, data sensitivity, and the total number of HVAs reported.

CISA identified that HVAs must conduct assessments every three years, by CISA itself for Tier 1 systems, and by a third-party assessor or by the agency itself for NT1 systems.[5] Additionally, assessors must be qualified by CISA. To that end, CISA created an Assessment Evaluation and Standardization (AES) program in 2019, and, through the General Services Administration's Highly Adaptive Cybersecurity Services program, began training vendors on its HVA assessments in late October 2021.[6]

Selecting or Becoming an NT1 HVA Assessor

NT1 systems have two options for assessments performed of their HVAs:

1. Select a team of internal personnel to attend CISA AES training and achieve qualification.
2. Hire a qualified third-party assessor to perform the assessments.

While there is no universally correct answer to which decision should be selected, following are a few considerations:

- Do you have the resources for a training?
- Do your resources have the necessary knowledge and experience to perform the assessments?
- Do your resources have the time to perform the assessment?

Additional information on becoming an HVA AES qualified assessor is available here.

[1]CIO.gov Handbook, accessed May 2, 2022, **https://www.cio.gov/handbook/policies-initiatives/high-value-assets/?clickEvt**.
[2]"High Value Asset Control Overlay: Version 2.0," Cybersecurity and Infrastructure Security Agency (CISA), accessed May 4, 2022, **https://www.cisa.gov/sites/default/files/publications/HVA%20Control%20Overlay%20v2.0_0.pdf**.
[3]"BINDING OPERATIONAL DIRECTIVE 18-02 - SECURING HIGH VALUE ASSETS," CISA, accessed May 2, 2022, **https://www.cisa.gov/binding-operational-directive-18-02**.
[4]The White House, December 10, 2018, accessed May 4, 2022, **https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf**.
[5]"DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed," United States Government Accountability Office, accessed May 4, 2022, **https://www.gao.gov/assets/710/704253.pdf**.
[6]Assessment Evaluation and Standardization (AES) page, accessed May 3, 2022, **https://www.cisa.gov/aes**.

Roles and Responsibilities

The HVA assessment team consists of three key assessor roles:

- Assessment Lead—Responsible for the overall assessment execution and team.
- Technical Lead—Responsible for technical review meetings and overall technical review.
- Operator—Responsible for leading the penetration-testing activities.

These roles may either consist of an individual who completes all activities associated with the role or of a team for larger systems.

Technical Considerations

The HVA assessment is not a controls-based review; rather, the assessment is based on core technical areas and generally consists of three core components:

1. Technical exchange meetings
2. Technical documentation review
3. Internal and external penetration testing

Preparing for an HVA Assessment

System personnel may be interested in performing actions to make sure their system is prepared for an HVA assessment. In order to prepare, you may consider:

- Contacting your agency HVA liaison for agency plans and for additional HVA resources.
- Performing a pre-assessment of your HVA to validate effectiveness of your security program. Even as a Tier 1 system, pre-assessments have been helpful.
- Contacting a qualified HVA AES assessor to help guide your organization through the requirements and necessary assessments.

Federal system personnel interested in learning more about HVAs or assessments should reach out to their agency HVA liaison.

About Guidehouse

Guidehouse is a leading consulting services provider, with 13,000 professionals in 50 locations globally. Ranked the 3rd-largest healthcare consulting firm in 2021 by Modern Healthcare, the Guidehouse Health team helps providers, government agencies, life sciences and retail companies, and payers solve their most complex issues and deliver innovative services to their communities.

Guidehouse has delivered cybersecurity solutions to commercial and public sector organizations, including Anthem, the Centers for Medicare & Medicaid Services, the Centers for Disease Control and Prevention, the National Institutes of Health, and multiple providers. Our team includes experts formerly responsible for protecting US national security systems against cyberthreats who guide clients through complex technology, business, and enterprise risk management scenarios. Our solutions help clients establish and optimize their information security and privacy operations to be better prepared to address current—and future—technology risks.

Guidehouse can help guide you through the HVA requirements

With one of the first fully qualified HVA assessment teams, Guidehouse's CISA-trained HVA NT1 assessors are ready to support your organization in HVA audit preparation and execution.

For more information, contact:

Dale Thornton
Director
dthornton@guidehouse.com

Phil Boone
Managing Consultant
phboone@guidehouse.com

Adam Simpkins
Managing Consultant
asimpkins@guidehouse.com