U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
National Risk Management Center
Washington, DC 20528

Pipeline Cybersecurity Assessments Update

ONG SCC / EGCC Meeting
July 9, 2020

Virtual Cybersecurity Assessments

CISA, as part of the Pipeline Cybersecurity Initiative (PCI), continues to work with the Transportation Security Administration (TSA) and pipeline owners and operators to conduct voluntary cybersecurity assessments. Recognizing the restrictions presented by the federal and private-sector response to COVID-19, CISA has adjusted procedures for the Validated Architecture Design Reviews (VADR) program in order to limit the need for on-site industry staff and enable both government and industry personnel to participate in the assessments virtually.

Virtual assessments include the same elements that make up a traditional VADR:

- Architecture Design Review,
- System Configuration and Log Review, and
- Network Traffic Analysis.

CISA works with participating companies to ensure that all sensitive information (i.e., network diagrams, packet capture data) is shared in a way that prioritizes the security of the information and the participating organization. Once it has securely received all information, CISA schedules interviews with key personnel using video-teleconference software (e.g., WebEx, Microsoft Teams). Interviews explore the same set of issues and questions that would be captured during a normal "in-person" assessment, and CISA breaks the engagement into a series of sessions over multiple days to accommodate irregular telework schedules and prevent extended screen sessions.

To date, the new "virtual" VADR program has been successfully demonstrated across multiple sectors, including pipeline owners and operators. Pipeline companies benefit from the assessments by building a better understanding the potential threats and vulnerabilities, and gaining insight into areas where cyber-preparedness can be improved within their systems. The assessments also help build lasting relationships with the federal cyber response community that can be leveraged during a cyber incident, should the need arise.

CISA will continue to offer the virtual assessments to pipeline stakeholders until such time when traditional, in-person assessments can resume safely. Until then, CISA encourages pipeline owners and operators to take advantage of the new service. For more information or questions on virtual VADRs, please visit CISA's website or email Central@CISA.gov. Organizations interested in scheduling an assessment are encouraged to email the TSA Surface Operations Pipeline Section (PipelineSecurity@tsa.dhs.gov).

Attachments:

- Pipeline Cyber Risk Mitigation Infographic (Final version, approved for release)
- VADR Fact Sheet

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

VALIDATED ARCHITECTURE DESIGN REVIEW

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Validated Architecture Design Review (VADR) is an assessment based on federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures.

CAPABILITIES

Architecture Design Review: In-depth review of network architecture design and interconnectivity to internal and external systems focused on defensive strategies.

System Configuration and Log Review: Detailed review of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies.

Network Traffic Analysis: Utilizes a combination of open-source and commercial tools to identify anomalous communications, which could indicate suspicious activity or misconfiguration.

ASSESSMENT OBJECTIVES

- Reduce risk to the Nation's critical infrastructure components.
- Analyze systems based on standards, guidelines, and best practices.
- Ensure effective defense-in-depth strategies.
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture.

ASSESSMENT TIMELINE

Pre-Planning

- Request VADR
- Sign and return documents
- Schedule Execution Activities
- Confirm Schedule

Planning

- Submit VADR specific documents and network diagram
- Schedule assessment planning meeting
- Submit network configurations, logs, and packet captures

- Interviews with key personnel

Execution

- Review submitted architecture
- Analyze packet captures

Post-Execution

- Out-brief – provides initial findings
- Final report (approximately 4 weeks)
- Follow-up on remediation actions – 180 days

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*