



CYBERSECURITY ASSESSMENTS

RULES OF ENGAGEMENT

Between the

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

And

February 12, 2024

Version – SLTT 5.10

Prepared By:

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

THE ATTACHED MATERIALS MAY CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY", OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE, INCLUDING CONFIDENTIAL AND LEGALLY PRIVILEGED INFORMATION UNDER FEDERAL AND STATE LAW. THE ATTACHED MATERIALS MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE PROTECTIONS FOR SUCH INFORMATION.



THIS PAGE INTENTIONALLY LEFT BLANK.



Table of Contents

1	Introduction	4
2	Procedures and Authorizations Prior to Service	4
3	Site Preparation	6
4	Assessment	9
5	Post-Assessment	10
6	Dispute Resolution	12
7	Amendment	12
8	Termination	12
9	Approval	12



1 Introduction

1.1 Purpose organization

This document establishes the Rules Of Engagement (ROE) for cybersecurity assessments requested by _____ (hereinafter, Entity) from the Cybersecurity and Infrastructure Security Agency (CISA).

1.2 Scope

This ROE applies to the Entity and CISA for all services documented through the procedures described herein. In addition, it applies to all CISA personnel who may access data obtained or generated under this ROE. This ROE does not include services for any classified computer, system, or network nor access to any classified information.

1.3 Background

CISA utilizes a defined strategy and methodology for testing, assessing, and analyzing target systems with state-of-the-art tools and highly trained security experts to conduct vulnerability and threat assessments. The purpose of these assessments is to assist the Entity in developing a strategy for improving cybersecurity posture and aligning it with enterprise architecture and mission objectives. CISA's assessment teams ("CISA Team") conduct comprehensive assessments of federal and non-federal networks, including critical infrastructure networks, under authority of Title XXII of the Homeland Security Act (6 U.S.C. § 651 et seq., *see especially* section 2209 (6 U.S.C. § 659)) and the Federal Information Security Modernization Act (FISMA) (44 U.S.C. §§ 3551 et al.). CISA Teams assess unclassified networks to evaluate the security posture when compared to best practices, regulations, policies, and standards relating to cybersecurity. CISA team services include various cybersecurity assessment activities such as network mapping, vulnerability scanning, host-based assessment, database and web application scanning, phishing, red teaming, and wireless access point detection. All services are fully described in Appendix C. The CISA Teams include both federal government employees and contractor support personnel. All contractors serving on CISA Teams have signed valid DHS 11000-6 Non-Disclosure Agreements.

2 Procedures and Authorizations Prior to Service

2.1 This ROE is effective when signed by the Entity CIO or equivalent authorized official and the CISA Assessments Chief.



- 2.2 Pursuant to this ROE, the Entity may request CISA team services that are described in Appendix C by completing an Appendix A in advance, each time service is requested. The CISA Team will only perform those services specifically selected by the Entity in the Appendix A and will only access systems and/or IP addresses identified by the Entity in the Appendix A, during the period of time agreed upon in that Appendix A. Each new Appendix A will be sequentially marked, e.g., Appendix A-1, Appendix A-2, Appendix A-3. The Appendix A is complete and becomes part of this ROE when all relevant information has been provided, including the selection of the Site Monitor, and Appendix A is signed by both the Site Authority (either the Site Monitor or the relevant CIO/authorized official) and the CISA Team Lead. Prior to the start of CISA team services, the Entity Site Monitor shall provide signed copies of the complete Appendix A to the Entity CIO or equivalent authorized official, and the CISA Team Lead shall provide the same to the CISA Assessments Chief.
- 2.3 In the event that any site/IP address proposed to be in-scope of requested CISA team services is operated by an Entity's sub-entity whose CIO or equivalent authorized official has unique or exclusive authority over that site/IP address, the sub-entity CIO or equivalent authorized official must complete and sign a separate Appendix A authorizing CISA to conduct requested services within that site/IP address range.
- 2.4 In the event that any site/IP address identified by the Entity in an Appendix A is operated or maintained by a third party (e.g. contractor or cloud-service provider) on behalf of the Entity, the Entity will ensure that the third party provides authorization for testing by either filling out and signing the form at Appendix B or completing the third party's authorization process and providing proof of authorization to the CISA Team. Appendix B is complete and becomes part of this ROE when signed by an authorized representative of the third party. Each new Appendix B will be labeled with the corresponding Appendix A number and a sequential alpha character. For example, an Appendix B for two third parties under the Entity's fourth request for services under Appendix A-4 would be labeled Appendix B-4a and Appendix B-4b, respectively. Prior to the start of CISA team services, signed copies of each complete Appendix B will be provided by the Site Authority to the Entity CIO or equivalent authorized official and by the CISA Team Lead to the CISA Assessments Chief.
- 2.5 Services provided by the CISA Team are described in the Services Catalogue at Appendix C. The Services Catalogue may be updated at any time by notice to the Entity. Correspondingly, the



template for Appendix A may be updated by notice to the Entity to reflect new or changed services offered by the CISA Team in an updated Services Catalogue.

- 2.6 Some CISA services described in the Appendix C Services Catalogue may require use of one or more of the Entity's unique seal, trademark, name, or insignia in phishing emails, phishing lures, and other techniques that will be made known to the Entity's Site Monitor, if utilized. The Entity hereby grants CISA the right to use such seal, trademark, name, or insignia solely for the purpose of preparing and sending phishing emails, phishing lures, and other techniques as part of the applicable services submitted by the Entity to CISA in an Appendix A. The Entity is responsible for obtaining any internal authorizations necessary for CISA use of its seal, trademark, name, or insignia, consistent with applicable law and procedures.
- 2.7 Some CISA services described in the Appendix C Services Catalogue will involve scanning or other network traffic originating from IP addresses or similar identifiers belonging to CISA or entities that CISA has contracted with, including cloud service providers. Such IP addresses or similar identifiers will be made known to the Site Monitor, when appropriate. CISA will also notify the Entity_ Site Monitor should the IP addresses or other identifiers change. In some instances (e.g., home users connecting to employer networks without a Virtual Private Network (VPN)), the Entity's network configuration may result in call-backs to CISA-controlled IPs addresses from Entity devices not utilizing the Entity's network resources. The Entity shall ensure its user agreements and computer/network terms of use policies account for and achieve consent to such callback activity to the greatest degree possible.
- 2.8 The Entity certifies that its log-on consent banners or notices; terms-of-use policies or user agreements; computer training programs; and any other mechanisms used to notify users and obtain their consent to the terms and conditions of computer use clearly demonstrate to Entity computer users and obtain their consent that:
- "Users have no reasonable expectation of privacy regarding communications or data transiting, stored on, or traveling to or from this network/system. Any communications or data transiting, stored on, or traveling to or from this network/system will be monitored and may be disclosed to third parties, including other governmental entities, or used for any lawful government purpose."
- For more information regarding legally sufficient log-on consent banners, see CISA's guidance here: <https://www.cisa.gov/publication/guidance-consent-banners>



- 2.9 The Entity agrees that for any vulnerabilities CISA may discover in commercial off the shelf products or services during the conduct of any assessment activities under this Rules of Engagement, CISA will manage such vulnerabilities and engage with the respective commercial product or service vendor consistent with CISA's publicly-available Coordinated Vulnerability Disclosure process described here: <https://www.cisa.gov/coordinated-vulnerability-disclosure-process>. Vulnerabilities identified in any non-commercially-available software or services are not subject to this clause, but will be submitted by CISA through any Entity vulnerability disclosure process, if available.
- 2.10 The Entity will ensure that access to the Entity data under this RoE is consistent with electronic communications privacy laws and other applicable laws, regulations, policies, and requirements of the Entity and any third parties and that data on the Entity systems and networks, which may be accessed by the CISA team under this RoE, has been obtained by the Entity in compliance with such laws, regulations, policies, and requirements.

3 Site Preparation

The Entity Site Monitor identified in Appendix A is an Entity authorized representative responsible for preparing the site, serving as the Entity's primary point of contact for the CISA Team, and monitoring CISA team services at that site for the agreed upon time and services identified in the Appendix A. Prior to the start of any services:

- 3.1 The Site Monitor and the CISA Team Lead will review the Appendix A and ensure that either an additional Appendix A and/or a completed Appendix B have been provided, if applicable, for all sub-entities or third parties.
- 3.2 The Site Monitor will coordinate and ensure, as appropriate, the involvement of Entity officials and adherence to Entity policies and standard operating procedures that could have an impact on the scanning activities and the information systems being assessed.
- 3.3 The Site Monitor will identify to the CISA Team potentially sensitive Entity devices prior to testing.
- 3.4 The Site Monitor is responsible for ensuring system backups have been performed and restore processes are validated prior to the start of external or internal CISA team services.
- 3.5 The Site Monitor will coordinate with and provide the CISA Team with information about the internal IT environment that is in-scope of the engagement.
- 3.6 Certain CISA team services may require administrator or other specific user access to the networks or systems being tested. The Site Monitor is responsible for ensuring access for the CISA Team,



when necessary. If administrator provisions are necessary, access may be granted by: (1) Either the Entity or CISA establishing a separate administrative account for testing (e.g., “CISATeam”), or (2) through the use, under Entity supervision and control, of an existing administrator account. It is recommended that separate testing accounts be established prior to the arrival of the CISA Team.

- 3.7 The Site Monitor, on behalf of the Entity and in coordination with other Entity officials as appropriate, will use reasonable efforts to identify to CISA in advance any categories of data, which may be encountered by CISA during the selected services, that are sensitive in nature or protected from disclosure by statute, regulation, or other authority, including personally identifiable information. the Entity will provide CISA instructions on how to identify and handle such data if encountered by the CISA Team. The Site Monitor and CISA Team Lead will work together to structure the engagement to ensure that the CISA Team does not come into contact with such data to the maximum extent possible or that appropriate data handling requirements have been put into place. The Site Monitor and CISA Team Lead will also discuss in advance what initial actions should be taken in the event that unforeseen sensitive data is encountered during CISA team services.
- 3.8 For assessments conducted onsite at the Entity facility, the Site Monitor may request and is permitted to authorize Entity IT staff or security personnel to scan the CISA Team assessment equipment for vulnerabilities prior to network connection using agreed upon vulnerability scanning tools. However, assessment equipment contains code and technical references which are not to be viewed, distributed or evaluated by external organizations. Under no circumstances will the CISA Team’s Government Funded Equipment (GFE) be relinquished from the control of the CISA Team.
- 3.9 The Site Monitor may request that the CISA Team conduct scanning activities on-site or remotely through a virtual private network.
- 3.10 For assessments conducted on-site at the Entity facility, the Site Monitor will provide to the CISA Team an on-site office or conference room-type workspace with AC power and a minimum of four internal network jacks/drops with a live connection. Personnel from Entity IT staff or security personnel are encouraged to observe the CISA Team on-site. If the CISA Team’s on-site access to an Entity facility requires agreement to or signature of any separate Entity policy relating to such access, the Entity **must** provide any such policies to CISA personnel for review at least 30 days prior to CISA’s date of arrival on-site. CISA personnel will typically not sign separate agreements, as this Rules of Engagement governs all assessment activities. Further, as there already exists both a statutory non-disclosure obligation covering federal employees at 18 U.S.C. § 1905 – the Federal Trade Secrets Act – and non-



disclosure obligations in this RoE (see Section 5 herein), CISA will not entertain signing separate agreements containing Non-Disclosure obligations.

3.11 For assessments conducted remotely, the Entity is responsible for providing a virtual private network connection. The Site Monitor will provide any information and support necessary for the CISA Team to connect remotely.

3.12 To prepare for and conduct certain assessments, the CISA Team may passively compile data from publicly-available and commercially-available resources, including information regarding the Entity's employees, network (e.g., registered network ranges and applications), and organization. CISA will delete this information, to the degree that it is not incorporated into the final report, upon completion of the selected assessment(s).

4 **Assessment**

During the assessment:

4.1 The CISA Team will use GFE, Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS), and open-sourced software and hardware. Use of any particular software or hardware by the CISA Team is not a government endorsement or sponsorship of any product, service, or company. CISA can furnish a brief description of any software or hardware used by the CISA Team in advance upon request.

4.2 The CISA Team will conduct any external assessment selected in Appendix A during the dates specified in Appendix A.

4.3 The CISA Team will conduct any internal assessment selected in Appendix A by connecting GFE to the Entity's network, either on-site or through a virtual private network provided by the Entity as determined by the Site Monitor, during the dates selected in Appendix A.

4.4 The CISA Team will collect and analyze data from Entity systems, networks, and processes to assess capability gaps in order to identify a road map for an enterprise-level risk-based mitigation strategy.

4.5 For on-site assessments, the CISA Team will provide to the Site Monitor a brief overview of daily activities and an out brief at the conclusion of the assessment.

4.6 The CISA Team Lead will notify the Entity's Site Monitor if a perceived significant event occurs during the assessment. The Site Monitor is responsible for having appropriate knowledge and understanding of the Entity networks and systems, identifying and/or confirming a significant event, and taking appropriate action, which may include suspension and/or termination of the assessment.



In the event a significant event occurs that warrants termination of the assessment, the CISA Team Lead and the Site Monitor will promptly provide to the Entity CIO or equivalent authorized official, the Entity Site Authority, and the CISA Assessments Chief a written account of the conditions and actions that led to the termination of the assessment. If the CISA Team Lead and Site Monitor cannot agree on the account, both accounts will be provided.

- 4.7 In the event a disagreement arises between the Entity and the CISA Team during the assessment, best efforts will be made to resolve such a disagreement at the lowest level possible.

5 Data Protection

- 5.1 Consistent with 5 U.S.C. § 552(b) and related law, CISA will not disclose under the Freedom of Information Act ("FOIA") any information provided by the Entity or collected by CISA under this ROE that is exempt from disclosure, which may include: Exemption (b)(3) as matters specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial information that is privileged or confidential, and Exemption (b)(7)(A)-(F) as records or information compiled for law enforcement purposes. Under Exemption (b)(4), CISA will assure, consistent with law, the confidentiality of any commercial or financial information the Entity identifies (including through the use of dissemination control markings) as information it customarily and actually treats as confidential.

- 5.2 Without limiting the previous paragraph, the Entity understands that CISA's obligations under the FOIA will apply to any written CISA notes of observations of Entity facilities and equipment (including computer screens); that CISA will make determinations regarding FOIA requests on a case by case basis consistent with its obligations under FOIA law, DHS and CISA FOIA regulations and policies, and its own internal guidance; and that any determinations regarding specific FOIA exemptions will be made at the time that the responsive records are processed. In accordance with 6 C.F.R. § 5.7, CISA shall promptly notify the Entity of any request for disclosure of confidential commercial information (as the term "confidential commercial information" is defined in 6 C.F.R. § 5.7(a)) provided by the Entity under this request and provide the Entity an opportunity to object to disclosure as provided by applicable law.

- 5.3 The Entity understands that information provided by the Entity that meets the definition of cyber threat indicator or defensive measure as defined in the Cybersecurity Information Sharing Act of 2015 (the "2015 Act"), 6 U.S.C. §§ 1501-1510, and that is provided in accordance with the 2015 Act's



requirements, will be protected as provided by the 2015 Act (including protection from release under FOIA). See the Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015 published by the Department of Homeland Security and the Department of Justice, available at <https://www.cisa.gov/automated-indicator-sharing-ais>.

- 5.4 The 2015 Act may offer disclosure protection for the final report when in the Entity's possession, as the 2015 Act provides a basis in federal law for state, tribal or local (STL) governments to exempt vulnerability information received from CISA from disclosure under any STL freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. See 6 U.S.C. § 1503(d)(4)(B). This exemption applies to a "cyber threat indicator or defensive measure;" the 2015 Act explicitly defines "cyber threat indicator" to include "a security vulnerability" (See 6 U.S.C. § 1501(6)(C)) and defines "defensive measure" to include any action, procedure, technique, or other measure to prevent or mitigate a known or suspected cybersecurity threat. See 6 U.S.C. § 1501(7)). SLT governmental entities, rather than CISA, are responsible for asserting this basis for withholding in response to any such requests under their own STL disclosure laws.
- 5.5 CISA may retain data submitted to or collected by CISA and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats. All data and assessment results may be anonymized and used to support trending analysis, which CISA may share publicly. Any data or assessment results used in trending status reports made publicly available will be non-attributable to the Entity.
- 5.6 CISA may share attributable summary participation and results information with other U.S. Federal Government entities with cybersecurity responsibilities, in a manner consistent with law and reasonably aimed at protecting from disclosure outside the U.S. Federal Government the identity and other information that is attributable or identifiable to the Entity. In this provision, "attributable summary participation and results information" is limited to the fact of the Entity's participation in particular CISA services covered by this RoE, summary results of any such CISA services provided to the Entity, and any associated CISA analysis and conclusions.
- 5.7 CISA agrees to reasonably and appropriately secure all data collected from the Entity's environment or as otherwise received or created in connection with the services provided to the Entity_. CISA agrees to keep all Entity Data confidential except as explicitly set forth herein and shall not otherwise use or disclose Entity Data except as provided herein. Any disclosures that occur outside



of the scope of this ROE shall be reported by CISA to the Entity. To the degree the Entity is subject to the Health Insurance Portability and Accountability Act (HIPAA), CISA agrees, as may be necessary for HIPAA compliance, to collaborate with the U.S. Department of Health and Human Services (HHS) for purposes of HHS determining the Entity's compliance with any applicable HIPAA requirements.

6 Post-Assessment

6.1 The CISA Team will provide the Entity with a final report within 30 days. The final report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in the final report or otherwise. The final report may include a Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.cisa.gov/tlp/>.

6.2 The Entity understands that it is under no obligation to implement any changes to its information systems that CISA may recommend and that CISA has not evaluated the feasibility or potential trade-offs associated with any such recommendations.

6.3 At some interval following the delivery of the final report, CISA may inquire with Entity personnel regarding the implementation status of any remediation or general security recommendations. Entity agrees to collaborate in good faith with such inquiries.

7 Dispute Resolution

Disputes will be resolved at the lowest level possible.

8 Amendment

Unless otherwise specified, this ROE may be amended by the mutual written agreement of the Entity CIO or equivalent authorized official and the CISA Assessment Chief at any time.

9 Termination

This ROE may be terminated either bilaterally by the mutual written agreement of the Entity CIO or equivalent authorized official and the CISA Assessments Chief at any time or unilaterally with thirty (30) days written notice. An assessment conducted under this RoE may be terminated unilaterally by either party at any time. If the Entity unilaterally terminates an on-site assessment, reasonable notice will be made to any on-site CISA personnel to allow CISA sufficient time to collect and remove any CISA equipment or materials from the premises.



10 Approval

By signing below, the approving the Entity official certifies the following:

- The Entity authorizes the CISA Team to provide services on Entity networks and systems as specified by the Entity in each Appendix A provided to CISA;
- The Entity has sufficient authority over or ownership of such networks and systems to authorize CISA to perform assessment activities on such networks and systems;
- The Entity agrees to obtain and provide to CISA a written authorization using the form at Appendix B from every third party that operates or maintains Entity networks/systems listed in each Appendix A;
- The Entity agrees to ensure that Entity network users have received notice and consent in accordance with this RoE, including paragraph 2.8;
- The Entity accepts that, while the CISA Team will use its best efforts to conduct its activities in a way that minimizes risk to Entity systems and networks, all of the assessment activities described above and in Appendix C, especially penetration testing or a red team assessment (if selected), create some risk to Entity systems and networks;
- The Entity accepts the risks to Entity systems and networks that may occur as a result of activities described in this RoE;
- The Entity acknowledges that CISA provides no warranties of any kind relating to any aspect of the assistance provided under this RoE;
- The Entity accepts the risk of any damage that may result from implementing any guidance provided by DHS; and
- The Entity has authorized you to make the above certifications on its behalf.

(Signature, Chief Information Officer or Equivalent)

(Date)

(Print Name and Title)

(Email and Telephone Number)

CISA Assessment Chief

(Date)

