CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY ASSESSMENTS

RULES OF ENGAGEMENT

Between the

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

And

April 02, 2019

Version – SLTT 4.00

Prepared By:

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

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

1 Introduction

1.1 Purpose organization

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

1.2 Scope

This ROE applies to _____ 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 Assessments utilize 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 _____ in developing a strategy for improving cybersecurity posture and aligning it with enterprise architecture and mission objectives.

CISA's Assessment teams 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 rogue wireless access point detection. 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.

Insert Establishment Background (Optional)

2 Procedures and Authorizations Prior to Service

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

2.2 Pursuant to this ROE, _____ may request CISA team services by completing an Appendix A in advance, each time service is requested. The CISA team will only perform those services specifically selected by _____ in the Appendix A and will only access systems and/or IP addresses identified by _____ 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 _____ Site Monitor shall provide signed copies of the complete Appendix A to the _____ 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 a _____ 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 _____ in an Appendix A is operated or maintained by a third party (e.g. contractor or cloud-service provider) on behalf of _____, _____ 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 _____'s fourth request for services would involve Appendix A-4 and 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 _____ 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 _____. Correspondingly, the template for Appendix A may be updated by notice to _____ 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 _____'s unique seal, trademark, name, or insignia in phishing emails. _____ hereby grants CISA the right to use such seal, trademark, name, or insignia. _____ 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 Site Monitor should the IP addresses or other identifiers change.

2.8 _____ 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 _____ 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."

3 **Site Preparation**

The _____ Site Monitor identified in Appendix A is an _____ authorized representative responsible for preparing the site, serving as _____'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 CISA team 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 _____ officials and adherence to _____ 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 _____ 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 provide the CISA team with information about the internal IT environment.

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. If administrator provisions are required, access will be granted by either (1)Either _____ or CISA establishing a separate administrative account for testing (e.g., "CISATeam"), or (2) through the use,

under _____ supervision and control, of an existing administrator account. It is recommended that separate testing accounts will be established prior to the arrival of the CISA team.

3.7 The Site Monitor, on behalf of _____ and in coordination with other _____ officials as appropriate, will use best 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, and 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 _____ facility, the Site Monitor may request and is permitted to authorize _____ 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 _____ facility, the Site Monitor will ensure that office or conference room-type workspace with AC power and a minimum four internal network jacks/drops with a live connection at the identified facility is available and provided to the CISA Team. Personnel from _____ IT staff or security personnel are encouraged to observe the CISA Team on-site.

3.11 For assessments conducted remotely, _____ 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 In order to prepare for and conduct certain assessments, the CISA Team may passively compile data from publicly-available and commercially-available resources, including information regarding _____'s employees, network (e.g., registered network ranges and applications), and organization.

This information, to the degree that it is not incorporated into the final report, will be deleted 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. A brief description of any software or hardware used by the CISA team can be furnished 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 _____'s network, either on-site or through a virtual private network provided by _____ as determined by the Site Monitor, during the dates selected in Appendix A.

4.4 The CISA team will collect and analyze data from _____ 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 outbrief at the conclusion of the assessment.

4.6 The CISA Team Lead will notify the _____ Site Monitor if a perceived significant event occurs during the assessment. The Site Monitor is responsible for having appropriate knowledge and understanding of the _____ networks and systems, identification and/or confirmation of 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 _____ CIO or equivalent authorized official, the _____ 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 _____ 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), CISA will not disclose under the Freedom of Information Act ("FOIA") any information provided by _____ under this request that is exempt from disclosure, including: 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.

5.2 Without limiting the previous sentence, _____ understands that this obligation will apply to any written CISA notes of observations of _____ 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, CISA FOIA regulations, 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. CISA shall provide _____ an opportunity to object to disclosure as provided by applicable law.

5.3 _____ understands that information provided by _____ 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.us-cert.gov/ais.

5.4 Further, the 2015 Act may offer disclosure protection for the final report when in _____'s possession, as the 2015 Act provides a basis in federal law for state, local, and territorial (SLT) 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)). STL 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 Collected data and assessment results may be anonymized and used to support government-wide trending analysis. Any data or assessment results used in trending status reports will be non-attributable to _____.

5.6 CISA will not share _____'s specific data and final report except as may be required by law.

6 **Post-Assessment**

6.1 The CISA team will provide _____ 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. Further dissemination of the final report may be governed by a Traffic Light Protocol (TLP) marking in the header, if present. For more information about TLP, see http://www.us-cert.gov/tlp/.

6.2 _____ understands that it is under no obligation to implement any changes to its information systems that CISA may recommend.

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 _____ 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 _____ CIO or equivalent authorized official and the CISA Assessments Chief at any time or unilaterally with thirty (30) days written notice.

10 **Approval**

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

- _____ authorizes the CISA team to provide services on _____ networks and systems in each Appendix A;
- _____ agrees to obtain and provide to CISA a written authorization using the form at Appendix B from every third party that operates or maintains _____ networks/systems listed in each Appendix A;
- _____ agrees to ensure that _____ network users have received notice and consent in accordance with this ROE;
- _____ accepts that, while the CISA team will use its best efforts to conduct its activities in a way that minimizes risk to _____ systems and networks, all of the tests described above,

and especially penetration testing or a red team assessment (if selected) create some risk to _____ systems and networks;

- _____ accepts the risks to _____ systems and networks that may occur as a result of activities described in this ROE;
- _____ acknowledges that CISA provides no warranties of any kind relating to any aspect of the assistance provided under this ROE;
- _____ accepts the risk of any damage that may result from implementing any guidance provided by DHS; and
- _____ 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)

For CISA Assessments Use Only – ROE S/N: