**MEMORANDUM OF UNDERSTANDING**

**BETWEEN**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**AND**

**IR Organization**

**FOR**

**cyber SECURITY ASSISTANCE**

This Memorandum of Understanding (MOU) is made between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and the IR Organization, to provide cyber security assistance.

**I. SCOPE OF WORK**

A. The IR Organization possesses the following network security capabilities listed in paragraph B. The network owner will initial and date next to each capability that the network owner wishes the IR Organization to exercise. The network owner can add additional capabilities without the necessity of a new MOU. The network owner may withdrawal a previously granted permission by 'lining through' the item and dating and initialing at the end of the individual task. Withdrawal of a previously granted permission does not require a new MOU.

B. Identification Tasks:

\_\_\_\_/\_\_\_\_ Assist Host and Service Enumeration

\_\_\_\_/\_\_\_\_ Create Active IP list

\_\_\_\_/\_\_\_\_ Active IP List on Key Parts

\_\_\_\_/\_\_\_\_ Scan ICS Equipment Parts

\_\_\_\_/\_\_\_\_ All Port Scan

\_\_\_\_/\_\_\_\_ List all AD Domain Accounts

\_\_\_\_/\_\_\_\_ Create firewall rule list

\_\_\_\_/\_\_\_\_ Deploy or evaluate host sensors

\_\_\_\_/\_\_\_\_ Deploy or evaluate NIDS

\_\_\_\_/\_\_\_\_ Establish network access accounts

\_\_\_\_/\_\_\_\_ Establish Mission log

\_\_\_\_/\_\_\_ Perform Vulnerability scan of network

\_\_\_\_/\_\_\_\_ DNS Host Name Mapping

\_\_\_\_/\_\_\_\_ Review Organizational User Policies

\_\_\_\_/\_\_\_\_ Gather AD Structure Information

\_\_\_\_/\_\_\_\_ Scan Device for Default Admin Password

\_\_\_\_/\_\_\_\_ Determine Installed Software

\_\_\_\_/\_\_\_\_ Perform STIG Scan

\_\_\_\_/\_\_\_\_ Perform Patch Compliance Scan

\_\_\_\_/\_\_\_\_ Perform SCAP Configuration Scan

\_\_\_\_/\_\_\_\_ Network owner authorizes all of the above Identify Tasks

Containment Tasks:

\_\_\_\_/\_\_\_\_ Export list of users from Domain Controller

\_\_\_\_/\_\_\_\_ Export groups from Domain Controller

\_\_\_\_/\_\_\_\_ Export Group Policy Objects from Domain Controller

\_\_\_\_/\_\_\_\_ Export Trust relationships from Domain Controller

\_\_\_\_/\_\_\_\_ Export OU structure from Domain Controller

\_\_\_\_/\_\_\_\_ Monitor AD new account creation

\_\_\_\_/\_\_\_\_ Monitor DHCP for new reservations

\_\_\_\_/\_\_\_\_ Monitor AD for new DHS names

\_\_\_\_/\_\_\_\_ Create team admin account in AD

\_\_\_\_/\_\_\_\_ Change local DC Administrator account

\_\_\_\_/\_\_\_\_ Disable local DC Administrator password

\_\_\_\_/\_\_\_\_ Change or disable Workstation local Administrator account

\_\_\_\_/\_\_\_\_ Verify patch compliance on all hosts

\_\_\_\_/\_\_\_\_\_ Network owner authorizes all of the above Protect Tasks

Eradication Tasks:

\_\_\_\_/\_\_\_\_ Synchronize all host clocks

\_\_\_\_/\_\_\_\_ Enable account usage auditing

\_\_\_\_/\_\_\_\_ Deploy network intrusion detection system

\_\_\_\_/\_\_\_\_ Monitor NIDS and Report threats

\_\_\_\_/\_\_\_\_ Investigate Alerts from host sensors

\_\_\_\_/\_\_\_\_ SIEM Events to IDS and network logs

\_\_\_\_/\_\_\_\_ Investigate unauthorized users or logins

\_\_\_\_/\_\_\_\_ Perform Rootkit check on host

\_\_\_\_/\_\_\_\_ host data collection windows

\_\_\_\_/\_\_\_\_ host data analysis registry autoruns

\_\_\_\_/\_\_\_\_ host data analysis security log

\_\_\_\_/\_\_\_\_ host data analysis installed software

\_\_\_\_/\_\_\_\_ host data analysis network connections

\_\_\_\_/\_\_\_\_ host date analysis processes

\_\_\_\_/\_\_\_\_ Network owners authorizes all of the above Tasks

\_\_\_\_/\_\_\_\_ Compare hashes of suspected malware

\_\_\_\_/\_\_\_\_ Perform manual host analysis – live system

\_\_\_\_/\_\_\_\_ Perform manual host analysis – memory image

\_\_\_\_/\_\_\_\_ Find and contain rogue workstations

\_\_\_\_/\_\_\_\_ Block unauthorized software

\_\_\_\_/\_\_\_\_ Stop credential re-use hack

\_\_\_\_/\_\_\_\_ Stop brute force hack

\_\_\_\_/\_\_\_\_ Stop malware rootkit

\_\_\_\_/\_\_\_\_ Stop data exfiltration

\_\_\_\_/\_\_\_\_ Stop malware backdoor

\_\_\_\_/\_\_\_\_ Stop C2 beaconing

\_\_\_\_/\_\_\_\_ Network owner authorizes all of the above Respond Tasks

Recovery Tasks:

\_\_\_\_/\_\_\_\_ Turn over incident-related documentation to network owner

\_\_\_\_/\_\_\_\_ Provide Vulnerability Assessment Scan to network owner

\_\_\_\_/\_\_\_\_ Provide improvement recommendations to network owner

\_\_\_\_/\_\_\_\_ Removal of tools, scripts software, and sensors

\_\_\_/\_\_\_\_\_ (Optional) Network owner request following tools left on network owner's

system: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_/\_\_\_\_ Networks owner authorizes all of the above Recovery Tasks

**II. CONFIDENTIALITY AGREEMENT**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and the IR Organization agree not to disclose each other's Confidential Information. Details of the Confidentiality Agreement are located in Appendix \_\_\_.

1. **LIABILITY**

In no event shall the IR Organization members providing support under this agreement or its members, agents, servants, independent contractors or suppliers be liable to the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ or any third parties affected by the services, support, or assistance provided by the IR Organization for any damages of any kind whatsoever, including, but without limitation, damages for loss of profits, business interruption, loss of information, disclosure of confidential or private information, or other losses, including pecuniary loss, arising out of services provided pursuant to this Agreement, or for special, indirect, consequential, incidental, or putative damages however caused, and regardless of the theory of liability, arising out of the services provided by the IR Organization.

1. **WARRANTIES**

Third Party Permissions and Authorizations. In the event that the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ uses equipment or software owned or operated by third parties, the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ represents and warrants that it has or will obtain authorization before the IR Organization provides any services or support as set forth in this document all licenses, authorizations and permissions from such third party entities as necessary. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ represents and warrants that all necessary notices have been given and all necessary permissions have been obtained and agrees to hold harmless the IR Organization members providing support under this agreement for any unauthorized use or access of equipment or software owned or operated by third parties.

1. **DISPUTES**

Should any terms in this agreement lead to a legal dispute, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and the IR Organization agree to bring this action before a forum in the State of <insert state>.

**VI. TERM**

This Agreement shall commence on the date this MOU is signed. This MOA will expire (1) at the request of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; or (2) when the IR Organization concludes that the mission is complete.

**VII**. **MODIFICATIONS TO THIS AGREEMENT**

Any amendments or changes to this to this MOA must be in writing and executed by all parties.

**VIII. TERMINATION**

Either party may terminate this MOU by giving written notice to all Parties. Early termination of support must provide a minimum of 48 hours’ notice, personally delivered or by email and fax. Such termination notice period shall not commence until receipt of delivery is obtained. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ shall not cut off **access to its system until** acknowledgment of such termination has been given, unless the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ reasonably believes immediate cut off of access is necessary to maintain the integrity of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ systems and ensure no interruption in the operations of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. As defined by The Adjutant General for the State of <insert state>, or his designee, in the event of military necessity, the State of <insert state> may terminate this agreement without written notice.

**IX.** **Contractual Rights**

This MOU does not create any explicit or implied contractual rights or obligations with respect to the signatory agencies.

**X. CONTACT PERSONS**

Contact Persons are listed in Appendix \_\_\_\_\_\_\_

**XI. REFERENCES**

References are listed in Appendix \_\_\_\_\_\_\_\_.

**XII. SIGNATORIES**

The undersigned Parties hereby acknowledge the foregoing as the terms and conditions of their understanding.

IR Organization**:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CEO (or designee) Date

**Network Owner:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**If on State Active Duty:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorized State Designee Date

APPENDIX \_\_\_

**Confidentiality Agreement**

1. The IR Organization agrees that it shall only use \_\_\_\_\_\_\_\_\_\_ Confidential Information, as defined below, for the purpose of providing agreed upon response capabilities. The IR Organization agrees that it shall use at least reasonable care to protect \_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information, as defined below. Except as otherwise provided in Paragraph 2, the IR Organization agrees that it shall not disclose to third parties \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ information including, but not limited to, proprietary information, market information, commercial information, critical infrastructure information, software information, systems information, personally identifiable information, technical data, and any other Networks information (“\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information”). The IR Organization agrees that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information shall not be disclosed and is exempt from disclosure pursuant to federal and state mandatory disclosure laws, including, but not limited to, the Freedom of Information Act,5 U.S.C. § 552.

2. Any \_\_\_\_\_\_\_\_\_\_\_ Confidential Information retained by the IR Organization will be returned to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and purged from the IR Organization systems after a formal request in writing is made by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to the IR Organization CEO, subject to litigation holds, preservation orders, or other lawful legal processes requiring the preservation of said data; provided, however, that any \_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information retained due to litigation holds, preservation orders, or other lawful legal processes requiring preservation of said data shall at all times remain subject to the terms of this MOU, and the IR Organization agrees to return to \_\_\_\_\_\_\_\_\_\_\_\_\_\_ and purge \_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information after the expiration of any such litigation hold, preservation order, or other lawful legal process requiring preservation of said data. Further, the IR Organization may retain one copy of \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information for archival purposes only, in accordance with the IR Organization standard and secure record retention policies, provided that any such archival copies shall at all times remain subject to the terms of this MOU.

3. Provided that the reports, statistical data, and other information do not identify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ or the Networks or are otherwise attributable to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ or the Networks, the IR Organization may (1) subject to the confidentiality obligations of this MOU, maintain reports, statistical data, and other information belonging to \_\_\_\_\_\_\_\_\_\_\_\_\_ for training, accounting, legal, and fiscal purposes; and (2) provide reports (oral and written) concerning any Incident Response Services provided to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (including but not limited to the types of intrusions, how the Networks were compromised, and probable targets) to federal and state agencies charged with national security, law enforcement, and cyber defense and protection.

4. IR Organization considers the Tactics, Techniques, and Procedures (TTPs) that it uses as Confidential Information and therefore subject to the same protections as the other Confidential Information outlined in this Appendix.

5. IR Organization will not agree to binding individual team members to a Confidentiality Agreement. IR Organization assumes responsibility for team members acting within the scope of their duties.

6. **OPTIONAL**. By initiating and dating this paragraph, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ consents that the IR Organization may share pertinent information with other states’ federal agencies, and military partners, including law enforcement agencies, when necessary to facilitate the IR Organization responsibilities pursuant to this MOU. National Guards, federal agencies, and military partners are, with respect to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information, subject to confidentiality obligations at least as restrictive as the ones set forth in this MOU, including the obligation to not disclose \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Confidential Information pursuant to federal and state mandatory disclosure laws. In the event that the IR Organization discovers a violation or potential violation of law by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, the IR Organization and the IR Organization HQ may provide information regarding and report that violation or potential violation of law enforcement agencies. (Initial\_\_\_\_\_\_\_\_\_\_ /Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_).

Appendix \_\_\_\_\_\_

Contact Persons

Team Lead

Assistant Team Lead

Appendix \_\_\_\_\_\_

References

NIST Cyber Security Framework

NIST 800-53 controls

NIST SP 800-184: Guide to Cyber Event Recovery

Freedom of Information Act, 5 U.S.C. § 552