



Wisconsin Cyber Response Team (CRT) Commitment Letter



Mission: To provide support for critical infrastructure in the state of Wisconsin in order to prevent, mitigate, and respond to cyber incidents through training, assessment, and response

Vision: Coordinated response effort from the State Volunteer Cyber Response Team (CRT) and National Guard, assisting in both preventing and responding effectively in the event of an emergency.

The CRT consists of volunteers from IT departments around the state trained in a variety of skillsets. The CRT typically responds to incidents that affect local or tribal governments primarily public entities (schools, utilities, etc.) or private sector entities providing a public-safety function. Recruitment is currently underway for the Cyber Response Team (CRT) coordinated by Wisconsin Emergency Management.



I understand that my role as a member of the Wisconsin Cyber Response Team (CRT) is a significant responsibility which I will make a priority when called upon. I also understand that deployments (virtual or on-site) may be at short notice and for extended periods of time. Further, I will:

- Support the mission, vision, values, and goals of the CRT and its sponsoring/host agency.
- Attend trainings, team meetings, and other mission-related coordination activities as reasonably possible.
- Complete independent study courses in a timely manner (e.g. IS-100, IS-200, etc.)
- Become a member of InfraGard.
- Ensure my sponsoring agency or primary employer is aware of the CRT commitment and has expressed support of my participation.
- I agree to inform my Team Lead, the CRT Director of Operations, and/or the Wisconsin Emergency Management Cyber Coordinator of any changes to this status or my ability to serve as a CRT member.
- Review and sign the Cyber Response Team Code of Conduct and Non-Disclosure Agreement.

Signed: _____

Print Name: _____

Date: _____

	Cyber Response Team Code of Conduct and Non-Disclosure Agreement	
---	---	---

Wisconsin Department of Military Affairs Appropriate Use Statement

All Wisconsin Cyber Response (CRT) Team equipment, systems, services, and software used during training, exercises, incident assessment, and response are intended only for the official business use of the State of Wisconsin. The State of Wisconsin reserves the right to audit, inspect, and disclose all transactions and data sent of this medium in a manner consistent with State and Federal laws. By using CRT systems, you expressly consent to all such auditing, inspection, and disclosure. Only software approved, scanned for virus, and licensed for State of Wisconsin use will be permitted on CRT systems. Any illegal or unauthorized use of State of Wisconsin CRT equipment, systems, services, or software by any person(s) may be subject to civil or criminal prosecution under state and federal laws and may result in disciplinary action where appropriate.

Initial Here _____

Cyber Response Team (CRT) Code of Ethical Practice

Duty of coordinated vulnerability disclosure

Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners, and users. Team members should coordinate with appropriate stakeholders to agree upon clear timelines and expectations for the release of information, providing enough details to allow users to evaluate their risk and take actionable defensive measures.

Initial Here _____

Duty of confidentiality

Team members have a duty to maintain confidentiality where appropriate. Requests to keep certain information in confidence may be made explicit, for example, with the Traffic Light Protocol (TLP). Team members should respect such requests whenever possible. If it

is not possible to keep information in confidence, for example, due to conflicts with the requirements of local laws, contracts, or a duty to inform, the Team member should inform the information owner of this conflict immediately.

Some duties of confidentiality are based on laws, regulations, or customs. If, during an incident response, some parties are bound by or expect confidentiality based on such considerations, they should do their best to make these expectations explicit in advance. All parties should then abide by the above expectation to maintain explicit requests to keep information in confidence when possible.

Initial Here _____

Duty to acknowledge

Teams receive information from many different sources: researchers, customers, other Teams, government entities, etc. Team members should respond to inquiries in a timely manner, even if it is only to confirm that the request has been received. When possible, Team members should set expectations for the next update.

Initial Here _____

Duty of authorization

Team members have a legitimate need and right to understand their areas of responsibility, acting only on systems that they are authorized to access. Team members need to be aware of how their actions may affect their constituents and ensure they do not cause additional harm while performing their duties. Where possible, constituents should be consulted before changes are made to their systems.

Initial Here _____

Duty to inform

Team members should consider it their duty to keep their constituents informed about current security threats and risks. When Team members have information that can either adversely affect or improve safety and security, they have a duty to inform relevant parties or others who can help, with appropriate effort, while duly considering confidentiality, privacy laws and regulations, and other obligations.

Initial Here _____

Duty to recognize jurisdictional boundaries

Team members should recognize and respect the jurisdictional boundaries, legal rights, rules, and authorities of the parties involved in activities related to incident response. Laws, regulations, and other legal issues, such as those related to privacy protection or data breach notifications, may differ between the involved jurisdictions. Jurisdictional

boundaries may be determined by the involved parties physical locations, such as their countries or domiciles, as well as by other factors concerning those parties. Even within a single country, laws and regulations may differ between political regions (e.g., between individual states in the USA) or between different businesses, industries, or sectors within that nation (e.g., healthcare, financial services and government facilities). National CSIRTs may have designated responsibilities and/or authority for activities involving constituents within their own jurisdiction, and they may also collaborate with or "hand off" information and activities to other entities that have authority for jurisdictions that cross boundaries. Team members should be aware of key issues that affect the jurisdictions involved, including but not limited to privacy regulations or data breach notification requirements. Because cybersecurity and privacy laws and regulations evolve and continue to be updated worldwide, it is advisable to consult with informed legal counsel for guidance whenever issues involve multiple jurisdictional boundaries.

Initial Here _____

Duty of evidence-based reasoning

Teams should operate on the basis of verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, Team members should provide evidence and scope transparently. If this is not possible, the reasons for not sharing this evidence and scope should be given with the information. Team members should refrain from spreading or sharing rumors. Any hypothesis should clearly be identified as such. Transparent evidence and reasoning processes are important even in the case of automated sharing, e.g., during automated sharing of large amounts of information. In this case, a description of the data mining process should be communicated at an intelligible level of detail.

Initial Here _____

Signed: _____

Print Name: _____

Date: _____

DEPARTMENT OF HOMELAND SECURITY

**NON-DISCLOSURE AGREEMENT FOR PROTECTED CRITICAL
INFRASTRUCTURE INFORMATION (PCII)**

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

I hereby acknowledge that I am familiar with, and I will comply with all requirements of the Protected Critical Infrastructure Information (PCII) program set out in the Critical Infrastructure Information Act of 2002 (CII Act), (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 U.S.C. 101 et seq.), as amended, the implementing regulations thereto (6 C.F.R. Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

I hereby acknowledge that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the PCII to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the PCII.

I understand and agree to the following terms and conditions of my access to PCII indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of PCII to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing PCII have been approved for access to it, and that I understand these procedures.
2. By being granted conditional access to PCII, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to PCII to which I am granted access.
3. I acknowledge that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with terms of this Agreement and the laws, regulations and/or directives, applicable to the information to which I am granted access. I understand that DHS may conduct inspections of my place of business pursuant to established procedures for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of PCII under this Agreement.

4. I will not disclose or release any PCII provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such PCII, I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the PCII. I will honor and comply with any and all dissemination restrictions cited to me by the proper authority.

5. (a) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or the Program Manager's designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(b) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same manner as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for PCII, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation that I have knowledge of, whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. With respect to PCII, I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this

Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783 (b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the brief officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

**DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT**

Acknowledgment

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:
---------------------	---	-------------------

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

Date:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:
---------------------	---	-------------------

Signature:

Date: