

Industrial Control Systems Joint Working Group Information Sharing Subgroup Charter

1. PURPOSE

1.1 Purpose Statement

The Information Sharing Subgroup has been established by members of the Industrial Control Systems Joint Working Group (ICSJWG), a cross-sector sponsored joint working group operating under the auspices and in full compliance with the regulatory requirements of the Critical Infrastructure Partnership Advisory Council (CIPAC). The purpose of the ICSJWG as described in the ICSJWG charter is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, and deployment of more secure control systems. Participants include international stakeholders, government, academia, owners/operators, systems integrators, and the vendor community. The Information Sharing Subgroup was formed to address challenges and priorities related to information sharing and the integration of control systems asset owners, operators, vendors and other stakeholders into a nationwide operational cyber risk management capability.

1.2 Challenges

As industrial control systems environments become increasingly interconnected, incident response and risk management capabilities have not kept pace in maturity to effectively manage cyber risk in control systems environments. The stakeholders involved in securing control systems throughout the product's life cycle face ongoing challenges with respect to awareness and availability of classified information and further dissemination to the private industry partners on a real-time basis.

1.3 Objectives

The Information Sharing Subgroup will develop recommendations to facilitate greater information sharing of vulnerabilities and threats to control systems among industry, vendors, and public sector. The subgroup will explore ideas and recommend methods to improve the vulnerability management processes across the industrial control systems landscape. The subgroup will provide input to incident reporting and handling guidelines in order to assist control systems owners and operators to respond to incidents as well as provide guidance for the development of methods to use lessons learned information toward prevention of reoccurrence or inadvertent introduction of new vulnerabilities.

2. OPERATING PRINCIPLES

The operating principles define and set forth how the group will operate including the authorities, duration, member roles and responsibilities, and the procedures it will follow to accomplish its purpose(s). The overarching ICSJWG statutes, requirements, and objectives as outlined in the ICSJWG charter will apply to and govern this subgroup.

2.1 Sponsorship and Authorities

The Information Sharing Subgroup is sponsored by the ICSJWG, and the subgroup derives its authority from both the ICSJWG charter and this subgroup charter. The requirements, stipulations, and authorizations of the ICSJWG charter are passed down and applicable to the members of this subgroup and its operation.

2.2 Subgroup Duration

The Information Sharing Subgroup initial period of performance will be 1 year from the date of execution of this charter by the ICSJWG and subgroup co-chairs. At the end of 1 year, the subgroup co-chairs and voting members may choose to extend the period of performance upon approval of ICSJWG co-chairs. The period of performance also may be terminated prior to the 1-year period if deliverables are completed and/or the ICSJWG co-chairs agree to dissolve the subgroup.

2.3 Membership

The ICSJWG is a collaborative and coordination body operating under CIPAC regulations. Members of the ICSJWG and attendees invited to participate as subject matter expert (SME) members derive no authority because of their participation in ICSJWG activities. Members of the subgroups will be selected from ICSJWG membership and from industry SMEs as follows:

2.3.1 Subgroup Co-Chairs

The subgroup will be lead by two subgroup co-chairs, one from the Sector Coordinating Council membership and one from the Government Coordinating Council membership as nominated by the ICSJWG and approved by the ICSJWG co-chairs. The two subgroup co-chairs shall act for the duration of this contract unless it is deemed necessary by the ICSJWG or co-chairs to nominate and appoint new subgroup co-chairs.



Industrial Control Systems Joint Working Group Information Sharing Subgroup Charter

2.3.1.1 Subgroup Co-Chairs Roles and Responsibilities:

- Draft, approve, and sign the subgroup charter with concurrence of the ICSJWG co-chairs.
- Recommend and vet subgroup membership and participant requests.
- Maintain the charter and ensure compliance by the subgroup membership and participants.
- Assign members and participants to perform specific tasks to complete the scope, deliverables, and products of the subgroup.
- Arrange and conduct meetings including documenting subsequent meeting minutes.
- Ensure that all meeting minutes are distributed to the subgroup membership, the ICSJWG co-chairs, and to the ICSJWG program office at icsjwg@dhs.gov.
- Review and approve products and deliverables with a simple majority concurrence of the subgroup membership.
- Report or provide status updates on the progress of the subgroup deliverables.
- Present deliverables and products to the ICSJWG co-chairs for acceptance.
- Recommend and perform updates to the goals and milestones of this charter as needed (with the approval of the ICSJWG co-chairs).
- Perform other duties as requested by the ICSJWG co-chairs.

2.3.2 Members

The subgroup will have at least three members in addition to the co-chairs. Members will be selected from the ICSJWG membership and from SMEs in academia, government, and industry based on their ability to contribute to the completion of the goals and milestones of the subgroup. The subgroup will endeavor to ensure that its membership is representative of the various critical infrastructure and key resource (CIKR) sectors as identified and recognized by the National Infrastructure Protection Plan.

Business of the subgroup will be conducted with a simple majority when voting is needed to resolve issues. The subgroup co-chairs will have the authority to break a tie. Members will assist with the development and approval of the products and deliverables of the subgroup.

2.3.2.1 Members Roles and Responsibilities:

- Complete tasks as assigned by the co-chairs.
- Attend meetings of the subgroup.
- Review and provide comments on products and deliverables.
- Vote on approval of products and deliverables.
- Comply with this charter and the regulations set forth in the ICSJWG charter.
- Ensure that the ICSJWG program office (icsjwg@dhs.gov) is copied on all written correspondence related to this subgroup.

2.3.3 SME Members

The subgroup co-chairs and members may choose to invite SME members on a task-by-task basis (in accordance with the ICSJWG charter) to contribute to the development of products or assist with specific tasks based on their expertise.

2.3.3.1 SME Member Roles and Responsibilities

- Comply with this charter and the regulations set forth in the ICSJWG charter.
- Complete tasks as assigned by the co-chairs and members.
- Attend subgroup meetings, as invited.

2.3.4 Executive Secretarial Support

Upon request, DHS will provide executive secretarial support to the subgroup co-chairs to perform administrative functions such as arranging for phone conference bridges, taking meeting notes, and notifying subgroup members of upcoming events.

2.4 Communication Protocols

This section provides the details for generating, sharing, and recording information about the subgroup's efforts and accomplishments:

2.4.1 Meetings

The subgroup will hold regular meetings where members and/or relevant SME members are invited to attend and engage in the specific tasks and goals of this charter. The subgroup may meet in a manner and frequency, as approved by the subgroup co-chairs, that is most conducive to completing the deliverables, addressing matters within the scope of the charter, and providing progress on the goals and milestones.

Industrial Control Systems Joint Working Group Information Sharing Subgroup Charter

Subgroup meetings may be called in accordance with the process identified in the ICSJWG charter, which includes the requirement to provide notice to the Designated Federal Official's (DFO) Compliance Liaison. All ICSJWG or subgroup meetings, conducted under the auspices of CIPAC, shall only be held when the CIPAC DFO designee, a DHS government official,^a is present.

If the subgroup meetings will or are expected to include both government and nongovernmental personnel and if the result will or might be characterized as a consensus endeavor, the meeting should be managed as a CIPAC meeting. Compliance for CIPAC regulatory obligations will be accomplished by DHS under the guidance of CIPAC DFO or the DFO designee.

2.4.2 Agendas and Meeting Minutes

As directed by the subgroup co-chairs, an agenda will be prepared for each meeting to identify the topics for review and the desired outcome of the meeting. At the conclusion of a meeting, minutes will be prepared to document the names of those in attendance and the decisions and actions agreed to. The agenda and subsequent meeting minutes will be distributed to members of the subgroup, the two ICSJWG co-chairs, and icsjwg@dhs.gov.

2.4.3 Review and Approval Process for Products and Deliverables

The subgroup will develop a method for its members to review and approve the deliverables that are completed to meet the goals and milestones of this charter. Deliverables approved by the subgroup membership will be forwarded to the ICSJWG co-chairs for acceptance and presentation to the ICSJWG membership at large.

2.4.4 Correspondence

All correspondence associated with subgroup business will be courtesy copied to icsjwg@dhs.gov.

2.4.5 Confidentiality

Members of the subgroup will keep the business and proceedings of all subgroup meetings confidential and will not disclose any information to organizations or individuals outside the membership of ICSJWG without approval from the subgroup and ICSJWG co-chairs. Subgroup members, however, may discuss their roles and activities of the

subgroup with their respective agencies or business units, provided such discussions are held as business sensitive.

2.5 Schedules and Reporting Progress

The subgroup will prepare and present progress reports at each ICSJWG general meeting or as directed by the ICSJWG co-chairs. The subgroup also will develop a schedule to identify each product or deliverable and the estimated dates for completing the milestones outlined in Section 3.0 of this charter.

3. OBJECTIVES, GOALS, AND MILESTONES

3.1 Objective 1—Develop recommendations to facilitate greater information sharing of vulnerabilities and threats to control systems among industry, vendors, and the public sector. Authorities responsible for the cyber risk management of CIKR industrial control systems must receive timely, actionable vulnerability and threat information in order to maintain an acceptable level of risk.

3.1.1 Goal 1: Identify current information sharing mechanisms and vehicles. Analyze for applicability and application to a centralized portal for vetting information and enhancing the level of confidence in situational awareness information.

3.1.2 Goal 2: Recommend improvements that address stakeholder equities and areas of concern. The stakeholders will be provided a direct line to present any topics that are deemed important toward the overall improvements in the private partnership arena.

3.1.3 Goal 3: ICS-CERT to integrate and facilitate improvements to processes based on input from Goals 1 and 2.

3.2 Objective 2—Improve the vulnerability disclosure/mitigation process across the industrial control systems (ICS) landscape. Participants in the vulnerability disclosure/mitigation process must be trusted and share vulnerability information in a timely manner in order to effectively mitigate the risk associated with vulnerabilities in industrial control systems.

3.2.1 Goal 1: Analyze the current state of vulnerability disclosure/mitigation and identify the gaps and challenges. This will allow for near-term improvements in information sharing and lead to timely implementation of protection strategies.

3.2.2 Goal 2: Document existing security mechanisms and work with the vendor subgroup to develop or clarify security procedures and performance expectations. This will assist asset owners to specify and procure built-in and

a. The DFO's Designee, also called the DFO Compliance Liaison, is a DHS government official who has been trained and certified by the CIPAC DFO to monitor, report, and ensure the regulatory compliance of any meeting held under the auspices of CIPAC.

Industrial Control Systems Joint Working Group

Information Sharing Subgroup Charter

effective security measures as they work with the ICS vendor community.

3.2.3 Goal 3: Evaluate the issue of vulnerabilities that occur at the component level or with third-party vendors and evaluate ways to improve the mitigation process. This will allow for consistent oversight toward ongoing protection effectiveness.

3.3 Objective 3—Create incident reporting and handling guidelines in order to assist owners/operators with responding to incidents. Industrial control systems asset owners/operators must be empowered with effective guidelines for reporting and handling cyber incidents in order to allow for timely assessments of developing cyber attacks on CI/KR, to allow for effective response efforts, and to manage risk strategically to CIKR.

3.3.1 Goal 1: Analyze sector specific concerns and evaluate if a one-size-fits-all approach is appropriate for all sectors. This will provide economy of scale as the applications of ICS are similar in many sectors, and some sectors have areas cross-cutting activities.

3.3.2 Goal 2: Develop a clear set of reporting and incident handling guidelines to help industry respond to incidents and understand the incident handling process.

3.4 List of Key Milestones

Key Milestones	Description	Due Date
Document current information sharing mechanisms and prepare recommendations and that address gaps	Objective 1, Goal 1, 2	180 days
Document existing vulnerability reporting procedures and deficiencies	Objective 2, Goal 1, 2	180 days
Prepare a recommendations guide for addressing gaps and improving vulnerability disclosure and mitigation	Objective 2, Goal 1, 2, 3	210 days
Develop a clear set of reporting and incident handling guidelines	Objective 3, Goal 1, 2	180 days