

ICSJWG and the CIKR ISE

Sharing Information across the Industrial Control Systems Joint Working Group

October 26, 2010



Homeland
Security

FOR OFFICIAL USE ONLY

Agenda

- Overview of the CIKR ISE
- Process Development Status
 - Next Steps
- HSIN-CS ICSJWG Portal Site Presentation
- HSIN-CS ICSJWG Membership Access



**Homeland
Security**

FOR OFFICIAL USE ONLY

Overview of the CIKR ISE



**Homeland
Security**

FOR OFFICIAL USE ONLY

Critical Infrastructure Key Resources Information Sharing Environment (CIKR ISE)

The CIKR ISE encompasses a comprehensive requirements collection process designed to collect address and track information sharing gaps or requirements across each of the five key development areas:

1. Policy & Governance

The foundational construct that defines the roles, responsibilities and processes for the sector.

2. Content

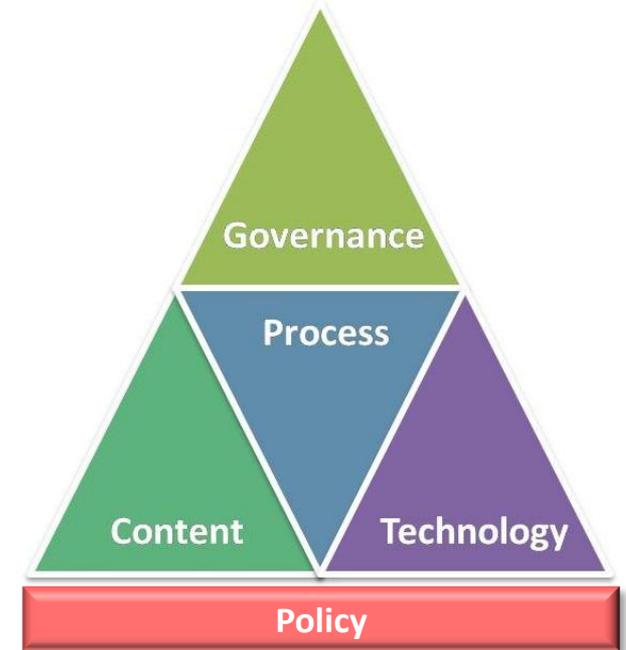
Formalized process that defines information that is required and generated by sector members.

3. Process

Core, enhanced and external procedures that define how a sector shares information.

4. Technology

Homeland Security Information Network – Critical Sectors (HSIN-CS) enables communication.



The ICSJWG focused on *Process*, *Content* and *Technology* to establish their CIKR ISE framework.



**Homeland
Security**

FOR OFFICIAL USE ONLY

Who are the CIKR?

CIKR SECTORS

- Chemical
- Commercial Facilities
- Critical Manufacturing
- Defense Industrial Base
- Energy (Dams, Nuclear, Electric, Oil & Natural Gas)
- Emergency Services
- Financial Services
- Food & Ag
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Nat'l Monuments & Icons
- Postal & Shipping
- Telecommunications
- Transportation
- Water



CIKR includes systems and assets so vital to the U.S. that their incapacitation or destruction would have a debilitating impact on national security, national economic security, public health or safety.

- Over 85 % of the nation's critical infrastructure is owned and operated by the private sector
- Successful Critical Infrastructure Protection (CIP) requires partnership and collaboration between the CIKR owners and operators and their federal, state, local, tribal and territorial government partners
- The CIKR ISE includes state and local fusion centers (e.g. NCRIC, NNCTC, etc.)

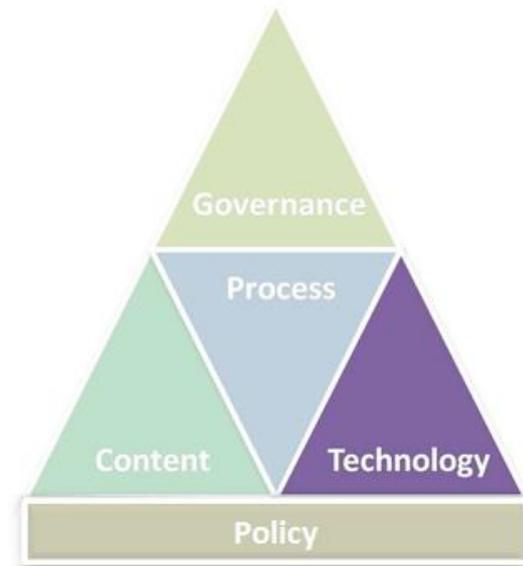


**Homeland
Security**

FOR OFFICIAL USE ONLY

HSIN-CS: Supporting the CIKR ISE

- The Homeland Security Information Network – Critical Sectors (HSIN-CS) provides the technological platform in which information sharing is enabled across 18 CIKR sectors and state and local fusion centers
- HSIN-CS is an information-sharing collaboration platform that incorporates multiple tools to provide tactical and planning functionality for owners and operators of critical infrastructure. These tools include:
 - Email Services
 - Web Conferencing
 - Document Management
 - Real-time Chat
 - Discussion Threads
 - Incident and Suspicious Activity Reporting
 - Situational Awareness



HSIN-CS is the technological platform that enables information sharing in the CIKR ISE at the national, state and local levels.



**Homeland
Security**

FOR OFFICIAL USE ONLY

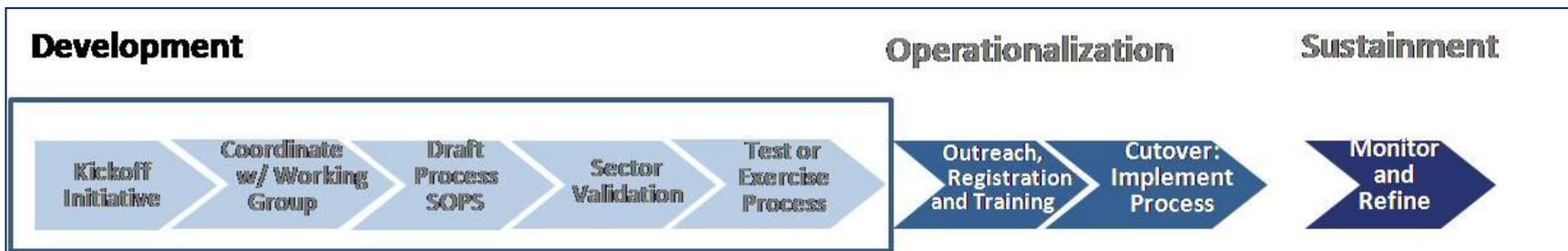
Process Development Status



**Homeland
Security**

FOR OFFICIAL USE ONLY

Process Development Methodology

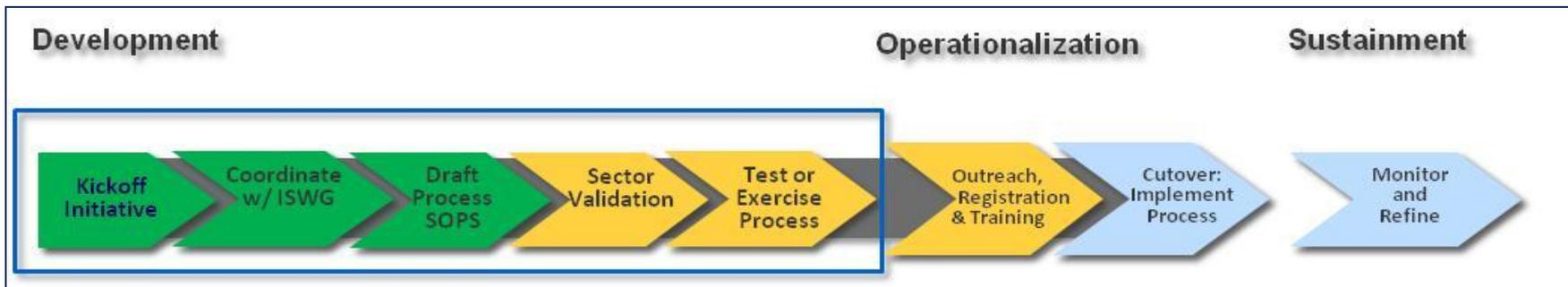


- The process development lifecycle includes the following steps:

1. **Kickoff** – Partnership and Outreach Division (POD), the POD Support Team and a lead representative from the ICSJWG will work together to initiate process development
2. **Coordinate** – The POD Support Team will facilitate sessions and work in coordination with ISWG subject matter experts to develop core information sharing capabilities / procedures that will be effective and sustainable for the ICSJWG
3. **Draft** – The POD Support Team will document existing processes and/or will provide best practice examples to the Working Group to facilitate developing information sharing and management processes and related requirements
4. **Validate** – The ICSJWG Information Sharing Working Group (ISWG) will review process document drafts to ensure the intent and mission interests of the Sector are fully incorporated within them
5. **Test or Exercise** – Test the process or apply it in an exercise or “pilot” environment to identify the need for any modifications



ICSJWG Process Development Status



▪ Next Steps:

- Continue to refine Standard Operating Procedures (SOPs)
 - Nomination/Validation and Data Management
- Add New Functionality as per Stakeholder Requirements
- Provide Continued Outreach to New Stakeholder Groups
- Provide Training Webinars to New Stakeholder Groups



HSIN-CS ICSJWG Portal Site Presentation



**Homeland
Security**

FOR OFFICIAL USE ONLY

HSIN-CS ICSJWG Membership Access

- Please forward all requests for access to HSIN-CS to **ICSJWG@dhs.gov**. Please include the requestors name, employer, work email address, and subgroup affiliation.
- HSIN-CS is available to qualified applicants who manage or directly support the operations of the nation's critical infrastructure listed in the table to the right. Each community within HSIN-CS, such as the CIKR sectors, state and local Fusion Centers, and cross-sector working groups, determines the membership criteria for its area.



**Homeland
Security**

FOR OFFICIAL USE ONLY



Homeland Security