

National Cybersecurity & Communications Integration Center (NCCIC)

W. Preston Werntz

Office of Cybersecurity and Communications (CS&C)

preston.werntz@dhs.gov

ICSJWG 2010 Spring Conference

Background

- The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resiliency and reliability of the nation's cyber and communications infrastructure.
- CS&C works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, economy, government services and the overall security of the United States.
- CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent and respond to cyber and communication incidents that could degrade or overwhelm these strategic assets.
- CS&C developed the National Cybersecurity & Communications Integration Center (NCCIC) to assist in this mission.

Recommendations

DHS Tiger Team Report (2007)

- The National Coordinating Center for Telecommunications (NCC) and the United States Computer Emergency Readiness Team (US-CERT) must ensure that their roles and responsibilities, relationships, information flow, and collaboration processes are coordinated.

GAO Report: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks (2008)

- DHS should define specific tasks and associated milestones for establishing the integrated operations center through merging NCC Watch and US-CERT and inviting and engaging key private sector critical infrastructure officials from additional sectors to participate in the operations of the new integrated center.

National Security Telecommunications Advisory Committee (NSTAC) Cybersecurity Collaboration Report (2009)

- Private sector should be elevated to the status of a trusted partner, and that the public and private sectors should share critical and time-sensitive threat information to strengthen the threat and warning architecture.

Vision

- NCCIC will improve the nation's capability and capacity to detect, prevent, respond, and mitigate disruptions of voice and cyber communications risks. NCCIC unifies vital IT and Communications operations centers thereby converging existing incident response mechanisms and better reflecting the reality of technological convergence.

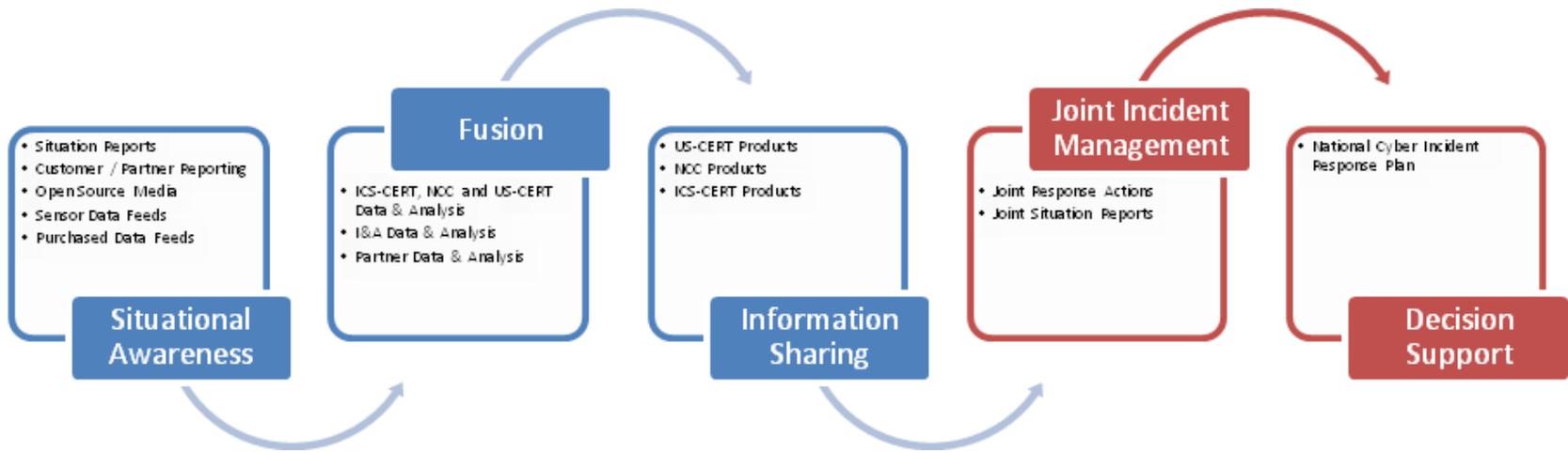
Operating Capability

- National-level operations center.
- Operates 24 hours/day, 7 days/week, 365 days a year.
- Conducts operations across different classification environments (e.g. Unclassified/FOUO, Secret, Top Secret-SCI).
- Static seating for over 60 personnel. Each workstation can have up to eight networks.
- Multiple conference rooms at different classification levels and call center.

Participants

- NCCIC is comprised of organizational components and operational liaisons.
 - Components refers to DHS organizations that have a major presence on the NCCIC floor, such as US-CERT, NCC, ICS-CERT, National Cyber Security Center (NCSC) and Office of Intelligence and Analysis (I&A).
 - Operational Liaisons refers to representatives from the federal departments and agencies, intelligence community, law enforcement, and private sector that participate in the NCCIC physically and/or virtually.
- While each component maintains their own operating mission, the execution of NCCIC's mission relies on coordinated operations that contribute to all products and services.

Operational Flow



- Operational rhythm for routine operations allows for real-time coordination and synchronization throughout the center, resulting in improved situational awareness
- Receive and fuse information from multiple sources and making that information actionable to reach a decision point
- Follow an altered operational rhythm during surge and incident management operations
- Data fusion occurs both on and off the floor (between analysis teams, I&A analysts and liaisons)
- Coordination with NCSC in support of their national mission.

Opening Day



Contacting the NCCIC

- Joint Duty Officer (JDO) - 703-235-8831 / 8830
- Senior Watch Officer (SWO) - 703-235-8832 / 8829

Components	Phone	Email (unclassified)
US-CERT Security Operations Center (SOC)	888-282-0870	soc@us-cert.gov
National Communications System (NCS)	703-235-5080	ncs@hq.dhs.gov
Intelligence and Analysis (I&A)	703-235-8836 / 8837	cyber@hq.dhs.gov
National Cybersecurity Center (NCSC)	TBD	TBD
Industrial Control System Cyber Emergency Response Team (ICS-CERT)	877-776-7585	ics-cert-soc@hq.dhs.gov



Homeland Security