APCO International

Public Safety Broadband Summit and Expo

Cybersecurity Panel

Mark Adams – Northrop Grumman

May 4-5, 2015 | Renaissance Hotel | Washington, DC

Whitehouse.Gov

FACT SHEET: Cyber Threat Intelligence Integration Center

Today, the President directed the Director of National Intelligence (DNI) to establish the Cyber Threat Intelligence Integration Center (CTIIC). The CTIIC will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats.

Office of Cybersecurity and Communications

The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.

US-CERT.GOV

US-CERT is part of DHS' National Cybersecurity and Communications Integration Center (NCCIC).

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a dynamic and complex environment.

Keys to the long-term Cybersecurity posture of FirstNet

- Awareness
- Planning
- Education

- Collaboration
- Standards
- Technology

Education – Representative Plan

- Public Safety Executive Course (Executives)
- Fundamentals of Cybersecurity (Everyone)
- Cyber Awareness for Mission Operations (Tactical)
- Network Cybersecurity Principals (IT)
- Mobile Security Principals (Mobile Users)