Homeland
Security

Updates to the NIST Cybersecurity Framework

NIST Cybersecurity Framework Overview and Other Documentation

October 2016

Agenda:

- **Overview of NIST Cybersecurity Framework**
- **Updates to the NIST Cybersecurity Framework**
- **DHS Critical Infrastructure Cyber Community (C3) Voluntary Program**
    1. ESS Roadmap to Secure Voice and Data Systems (2014)
    2. ESS Cybersecurity Framework Implementation Guidance (2015)
- **Additional Cybersecurity Guidance and Resources**

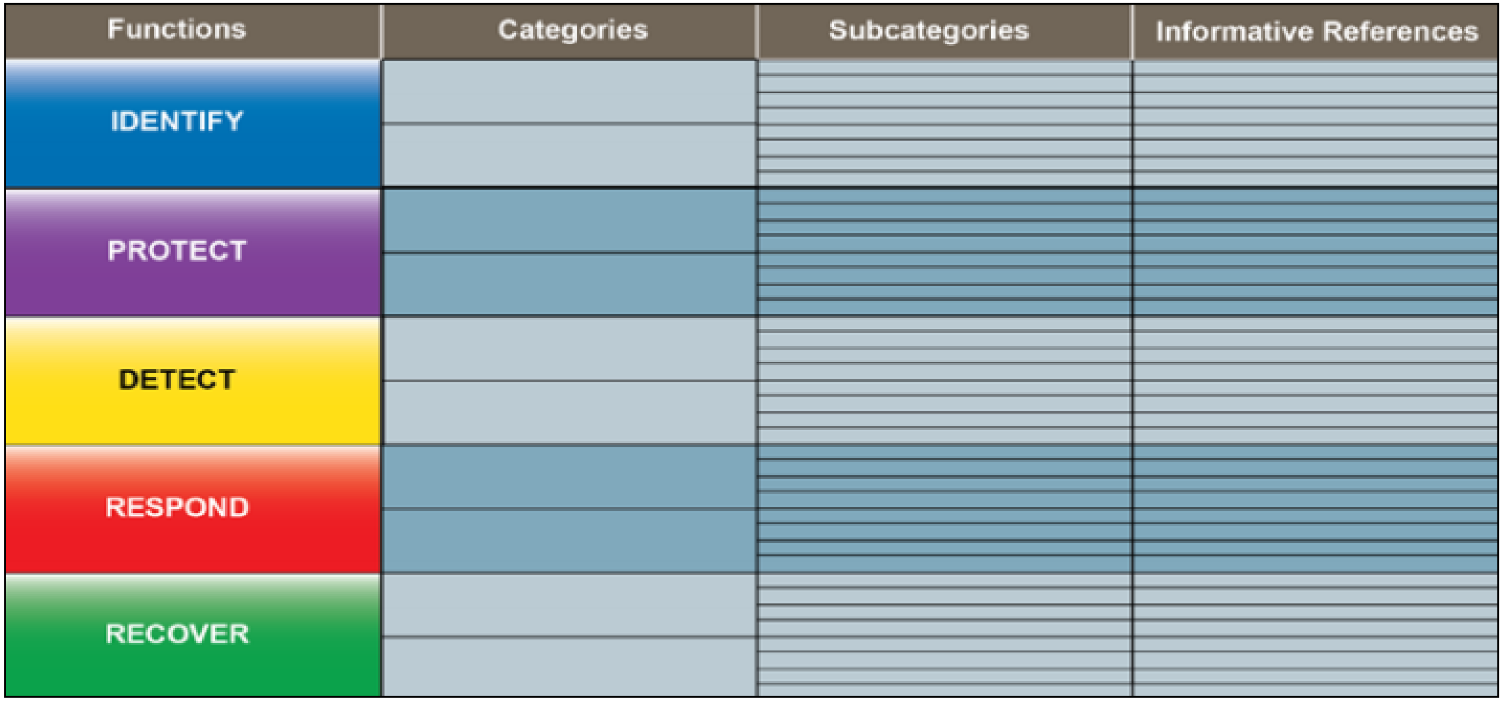
NIST Cybersecurity Framework

- Released in February 2014, the NIST Cybersecurity Framework (CSF) is a flexible, voluntary risk-based approach to improving the security of critical infrastructure
- Collaboratively developed between government and the private sector, based on industry standards and best practices
- Designed to complement existing cybersecurity risk management process or to develop a credible program if one does not exist
- Repeatable process to identify and prioritize cybersecurity improvements and maximize investment in mitigations
- Can be used by any organization – regardless of size or industry sector – based on their unique risks and business needs

For more information on the CSF: https://www.nist.gov/cyberframework

Using the NIST Cybersecurity Framework – Core

- Organizes cybersecurity activities into five functions
  - Each function has objectives arranged in categories and subcategories, which each map to a list of industry best practices and standards that should be used to achieve those objectives.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Using the NIST Cybersecurity Framework – Example

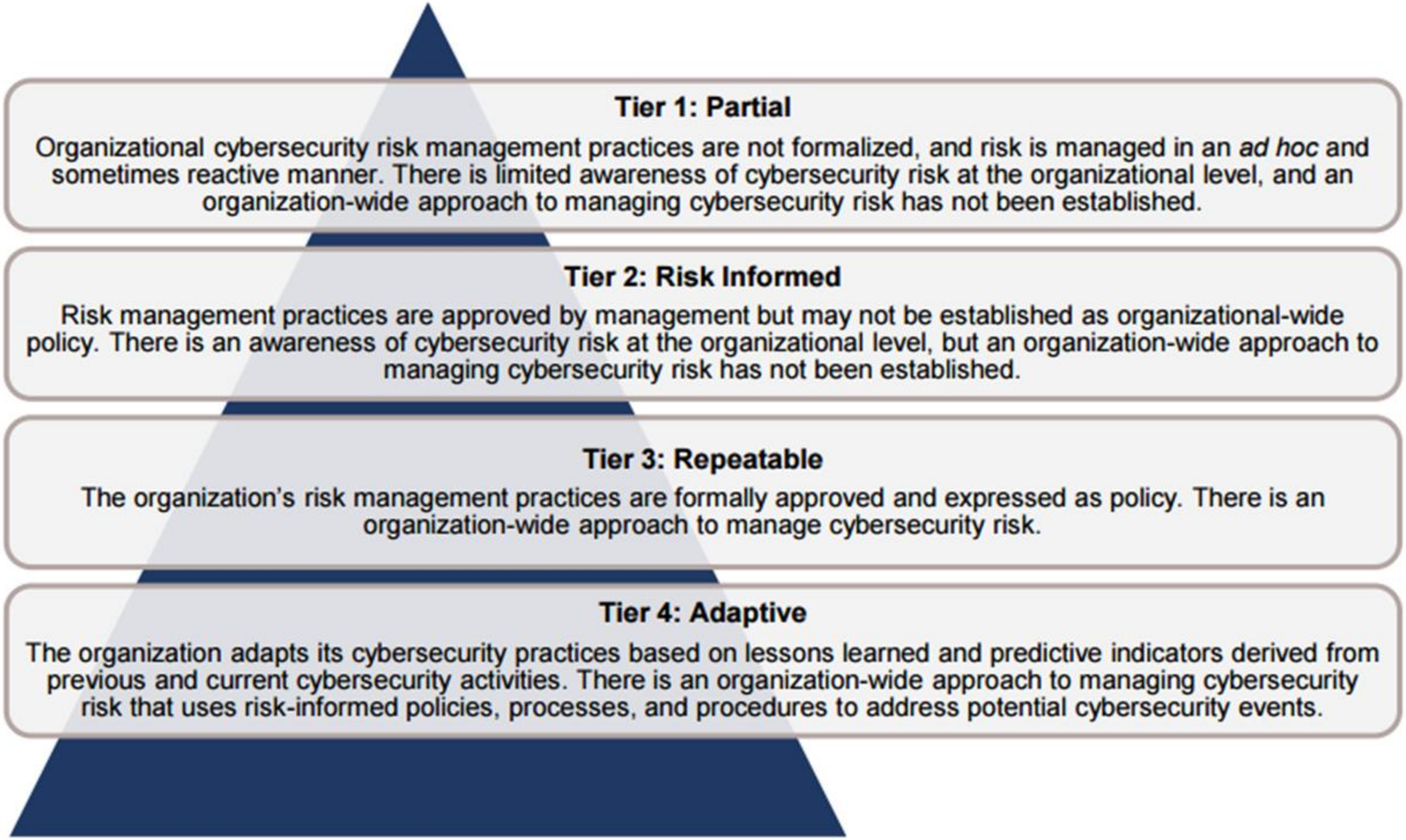
Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8

What to Do

Information that can help to achieve it

Using the NIST Cybersecurity Framework – Tiers

- Provide context for how an organization views cybersecurity risk and the processes in place to handle the risks



Tier 1: Partial

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk Informed

Risk management practices are approved by management but may not be established as organizational-wide policy. There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.

Tier 3: Repeatable

The organization's risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.

Tier 4: Adaptive

The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

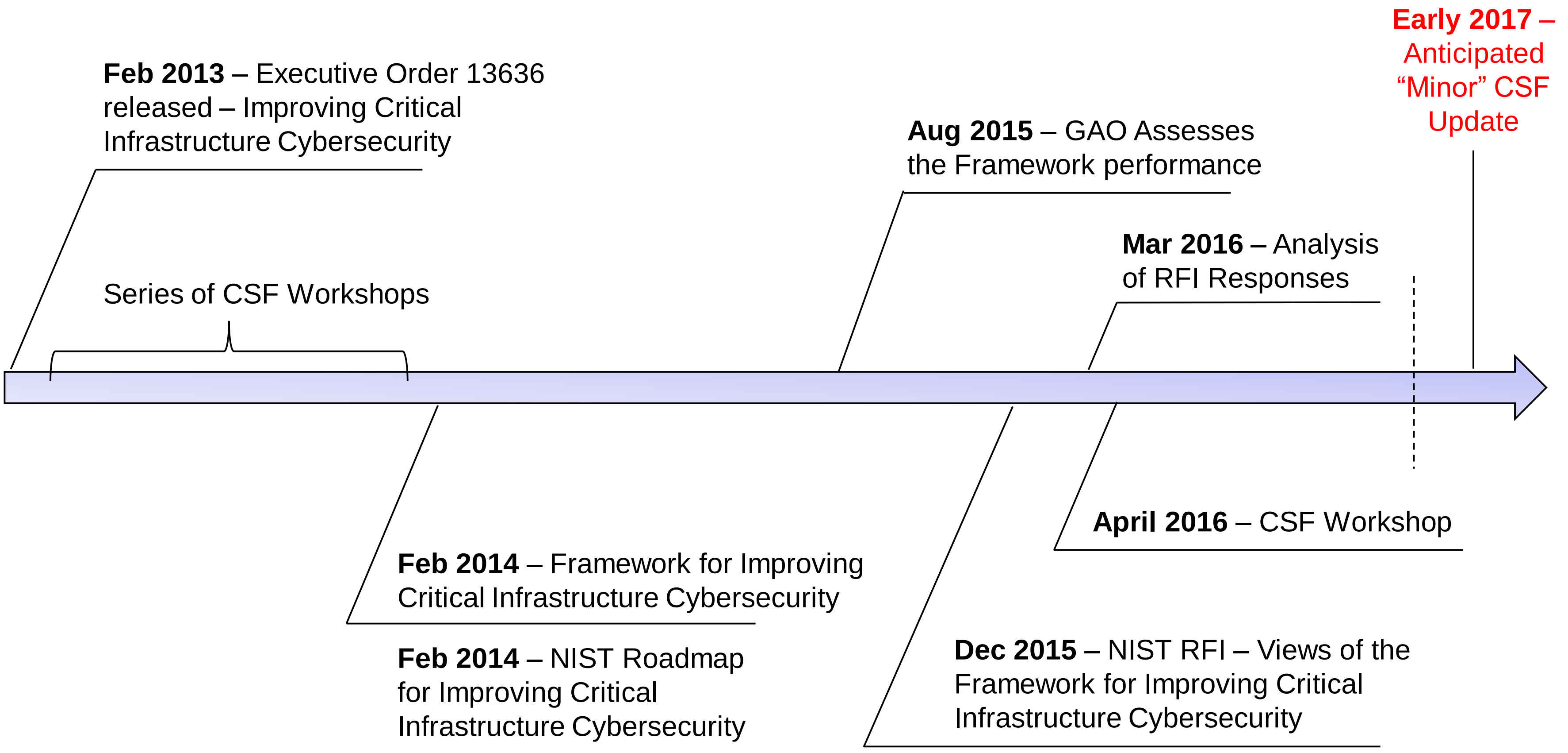
Source: ESS Framework Implementation Guide, 2015

Using the NIST Cybersecurity Framework – Process

- The CSF suggests a seven-step process to help organizations create a new cybersecurity program or improve an existing program
    - Step 1: Prioritize and Scope
    - Step 2: Orient
    - Step 3: Create a Current Profile
    - Step 4: Conduct a Risk Assessment
    - Step 5: Create a Target Profile
    - Step 6: Determine, Analyze, and Prioritize Gaps
    - Step 7: Implement Action Plan

Source: ESS Framework Implementation Guide, 2015

NIST CSF Timeline



Feb 2013 – Executive Order 13636 released – Improving Critical Infrastructure Cybersecurity

Series of CSF Workshops

Feb 2014 – Framework for Improving Critical Infrastructure Cybersecurity

Feb 2014 – NIST Roadmap for Improving Critical Infrastructure Cybersecurity

Aug 2015 – GAO Assesses the Framework performance

Dec 2015 – NIST RFI – Views of the Framework for Improving Critical Infrastructure Cybersecurity

Mar 2016 – Analysis of RFI Responses

April 2016 – CSF Workshop

Early 2017 – Anticipated “Minor” CSF Update

Updates to the NIST Cybersecurity Framework

- 105 Responses
- Wide variety of respondents
  - Local government
  - State government
  - Federal government
  - Educational institutions
  - Critical infrastructure and other industry partners
    - Chemical
    - Communications
    - Critical Manufacturing
    - Defense
    - Emergency
    - Energy
    - Financial
    - Food/Agriculture
    - Government Facilities
    - Healthcare
    - Information Technology
    - Water
  - Industry associations and trade groups
  - International perspectives

Updates to the NIST Cybersecurity Framework

Theme	Description
Framework Update Timeline	There were diverse comments on whether an update is necessary or desirable.
Update to Framework Content	Many respondents had specific suggestions of ways to update and expand the Framework.
Update Process	The Framework should be updated through a collaborative process and with minimal disruption to current industry use.
Framework Governance	Respondents are comfortable with NIST's continued leadership in the Framework process, though transition should be considered at a later date.
Optimal Industry Leadership	Any possible future steward of the Framework should be a respected, internationally-recognized, neutral, 3rd party organization.
Industry Resources	Industry resources are useful but additional guidance is needed, especially for small and medium-sized businesses.
Challenges in Sharing Best Practices	There is a need for additional sharing of best practices surrounding use of the Framework.
Regulation	Many users of the Framework say that regulation is a necessary consideration in the development of their cybersecurity programs and caution about the potential negative impact of additional regulatory requirements.
International Alignment	The Framework is gaining traction internationally, but still needs continued outreach.
Awareness	Much progress has been made in spreading Framework awareness, but more is still needed.

Source: *Analysis of Cybersecurity Framework RFI Responses*, NIST, March 24, 2016

Updates to the NIST Cybersecurity Framework

- Minimal disruption
- Clarifying and refining of current Framework attributes
  - Update Informative References
  - Clarify guidance for Implementation Tiers
  - Review placement of cyber threat intelligence in the Core
  - Provide guidance for applying the Framework to supply chain risk management
- Potential draft for comments "early calendar year 2017"
- Other products may be modified as well:
  - NIST Roadmap for Improving Critical Infrastructure Cybersecurity
  - Frequently asked questions (FAQs)
  - Publications, such as those hosted at the Computer Security Resource Center (CSRC)

Updates to the NIST Cybersecurity Framework

- Related efforts
  - Framework governance methodology
    - Describe stakeholder roles in the Framework ecosystem
    - Establish approximate timelines for future Framework updates
    - Define the difference between a “major” and “minor” update
  - Self-assessment criteria
    - Support organizational understanding of cybersecurity risk management business practices
    - Based on Framework and key concepts from the Baldrige Performance Excellence Program
      - 9/15/2016 NIST Releases Baldrige-Based Tool for Cybersecurity Excellence; Comments Sought on Draft Guide to Enhance Cybersecurity Framework

        https://www.nist.gov/news-events/news/2016/09/nist-releases-baldrige-based-tool-cybersecurity-excellence
  - Continued outreach efforts
    - International
    - Small and medium-sized businesses
    - Regulators

Critical Infrastructure Cyber Community (C³) Voluntary Program

- DHS CS&C is the coordination point for promoting implementation of the Framework
- Three main activities
  - **Use:** Promote understanding and support development of guidance to use the Framework
  - **Outreach and Communications:** Connect stakeholders and guide organizations to resources
  - **Feedback:** Solicit feedback on how Framework is used and recommendations for improvements
- Implementation guidance
  - General guidance on how the Framework applies to critical infrastructure sectors and organizations
  - Tailored guidance specific to sectors, including the Emergency Support Services (ESS) sector
- 2014 – *ESS Roadmap to Secure Voice and Data Systems*

  https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data%20Systems-508.pdf
- 2015 – *ESS Cybersecurity Framework Implementation Guidance*

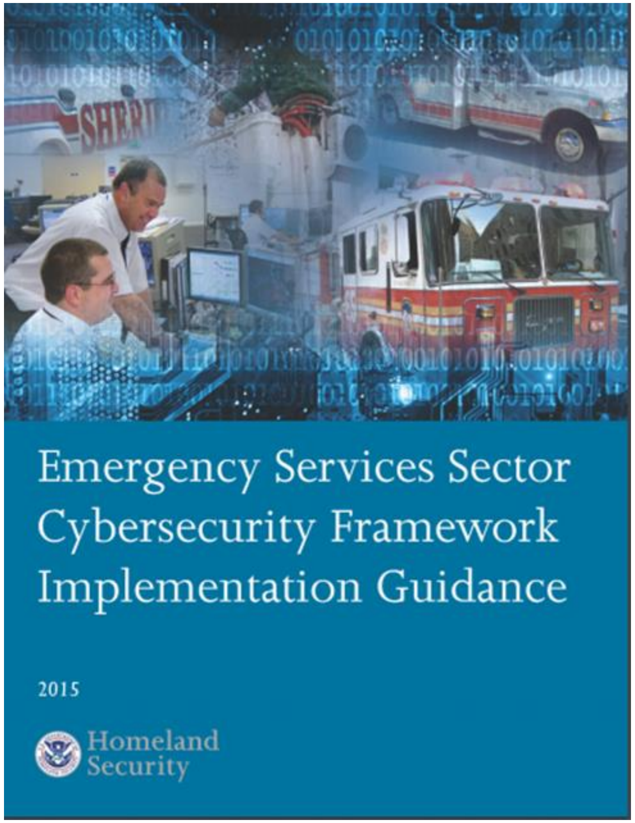
  https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/ess-framework-implementation-guide-2015-508.pdf

ESS Roadmap to Secure Voice and Data Systems (2014)

- In 2012 the *ESS Cyber Risk Assessment* (ESS-CRA) identified operational and strategic risks to ESS infrastructure
- The *Roadmap* identifies and discusses several proposed risk mitigation measures and includes:
  - justification for the response,
  - sector context,
  - barriers to implementation, and
  - suggestions for implementation
- Designed to help ESS personnel understand how to organize and conquer risk mitigation measures, it uses language from the NIMS/Incident Command System to help delineate responsibilities
- Guidance provided in the Roadmap may apply to any public safety cyber resource

ESS Cybersecurity Framework Implementation Guidance (2015)

- In response to the NIST CSF, DHS, as the Sector-Specific Agency (SSA), worked with the ESS Coordinating Council (SCC) and Government Coordinating Council (GCC) to develop this Implementation Guidance specifically for ESS organizations
- The Implementation Guidance provides ESS organizations with:
  - Background on the Framework terminology, concepts, and benefits of its use;
  - A mapping of existing cybersecurity tools and resources used in the ESS that can support Framework implementation; and
  - Detailed Framework implementation steps tailored for ESS organizations
  - A notional use-case study



Emergency Services Sector Cybersecurity Framework Implementation Guidance

2015

Homeland Security

Implementation Guidance – Mapping

- Additional pre-existing cybersecurity guidance, tools and resources of the ESS community are mapped as part of the Implementation Guidance:
  - Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program
  - Cyber Resilience Review (CRR)
  - Cybersecurity Evaluation Tool (CSET)
  - Emergency Services Sector Cyber Risk Assessment (ESS-CRA)
  - ESS Roadmap to Secure Voice and Data Systems (Roadmap)
  - Emergency Services Sector-Specific Tabletop Exercise Program (ES SSTEP)
  - Health Insurance Portability and Accountability Act (HIPAA)

Function	Category	Subcategory	CRR	CSET	ESS-CRA	ES SSTEP	Road-map	HIPAA	Energy C2M2
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	X	X	X		X	X	X

Additional Cybersecurity Guidance and Resources

- OEC Fiscal Year 2016 SAFECOM Guidance on Emergency Communications Grants

  https://www.dhs.gov/sites/default/files/publications/FY%202016%20SAFECOM%20Guidance%20FINAL%20508C.pdf

- Appendix B – Technology and Equipment Standards
  - Cybersecurity for Emergency Communications
    - Review of Cyber Risks
    - Cybersecurity Best Practices
    - Standards for Cybersecurity
    - Cybersecurity Resources

Resources

Additional Guidance

Homeland Security
SANS
CNSS
ITU
911.gov
atis
THE WHITE HOUSE WASHINGTON
FCC
NIST National Institute of Standards and Technology U.S. Department of Commerce
NENA THE 9·1·1 ASSOCIATION

Contact Information

- Robert “Dusty” Rhoads
  - U.S. Department of Homeland Security, Office of Emergency Communications
  - Branch Chief
  - Robert.Rhoads@HQ.DHS.GOV
  - (703) 235-4014