

## *IMPLEMENTING THE NECP WEBINARS*

# HOW DOES YOUR AGENCY IMPROVE ITS CYBERSECURITY POSTURE? IMPLEMENT THE NIST CYBERSECURITY FRAMEWORK

JULY 2020



# Agenda

- **Webinar Overview and Objectives**
- **National Emergency Communications Plan (NECP) and SAFECOM Nationwide Survey (SNS): Cybersecurity**
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
- **Resources and Actions**
- **Question and Answer Session**



# Webinar Objectives

- Discuss the impact of cybersecurity on emergency communications
- Use the NECP to learn practical solutions to enhance cybersecurity risk management practices
- Gain an understanding of how to implement the NIST Cybersecurity Framework to mitigate cyber risk
- Provide links to CISA Central and other CISA resources you can use to mitigate cyber risk



# Presenters

**Katharine Willers**

Emergency Communications

Cybersecurity and Infrastructure Security Agency



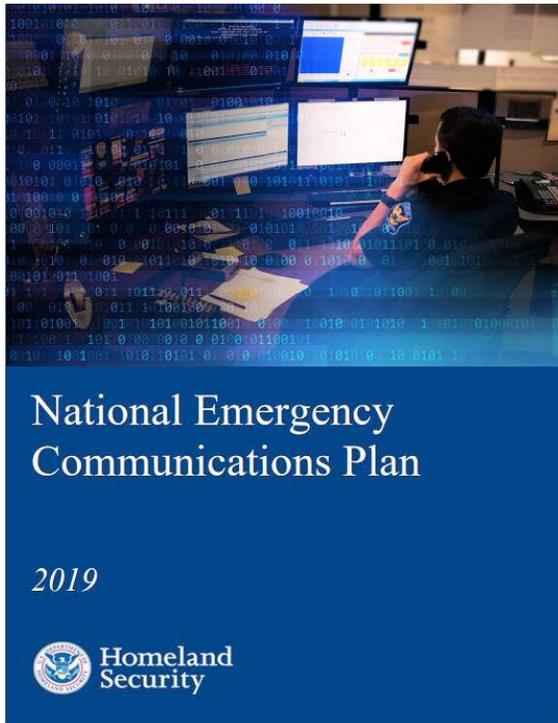
**Amy Mahn**

Applied Cybersecurity Division

National Institute of Standards and Technology



# National Emergency Communications Plan



Mandated by Title XVIII of the Homeland Security Act of 2002, the NECP was first published in 2008, and its latest update was published in 2019.



The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities.



The Plan is designed to provide guidance to those that plan for, coordinate, maintain, invest in, and use communications to support public safety operations.



It helps stakeholders enhance and update the policies, governance structures, planning, and protocols that enable responders to communicate and share information under all circumstances.



The NECP navigates the complex mission of maintaining and improving emergency communications while also integrating new technologies and capabilities for emergency responders.



# NECP Goals

**NECP Vision:** To enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event



## Goal 1: Governance and Leadership

Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem



## Goal 2: Planning and Procedures

Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem



## Goal 3: Training, Exercises, and Evaluation

Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies



## Goal 4: Communications Coordination

Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events



## Goal 5: Technology and Infrastructure

Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely



## Goal 6: Cybersecurity

Strengthen the cybersecurity posture of the Emergency Communications Ecosystem



# Cybersecurity Overview

- Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and the public
- Cyber threats are now more complex and sophisticated and have become one of public safety's greatest operational risks
- The number of incidents is on the rise with significant consequences on emergency communications systems
- The SNS found that 37% of public safety organizations have been impacted by a cybersecurity disruption



## Public Safety Cyber Incidents

- ***Madison, Wisconsin Distributed Denial-of-Service Attack*** - the city's internet-connected emergency communications system was crippled which impeded emergency responders' ability to connect to the 9-1-1 Center and slowed down the system used to automatically dispatch responders to emergencies.
- ***Texas Ransomware Attack*** - more than 20 entities (mostly small, rural local governments) were hit with a ransomware attack; the victims were able to recognize the incident as ransomware and self-reported the attacks, resulting in a successful coordinated state and federal response

# SAFECOM Nationwide Survey

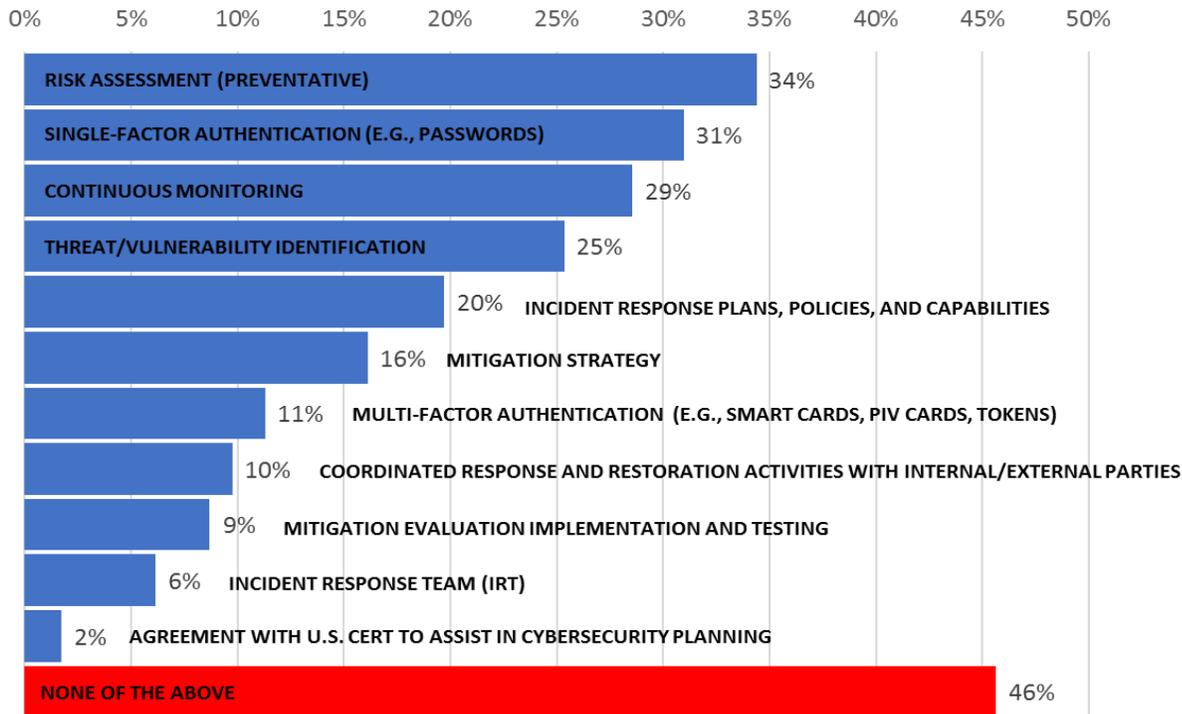


- The 2018 SNS was a data collection initiative that supported the content and recommendations of the NECP
- The SNS consisted of 38 questions that span the 5 elements of the *SAFECOM Interoperability Continuum*, plus a security element that accounted for cybersecurity
- Findings from the SNS gauge the status of the Nation's emergency communications capabilities and helped inform the NECP's goals, objectives, and success indicators

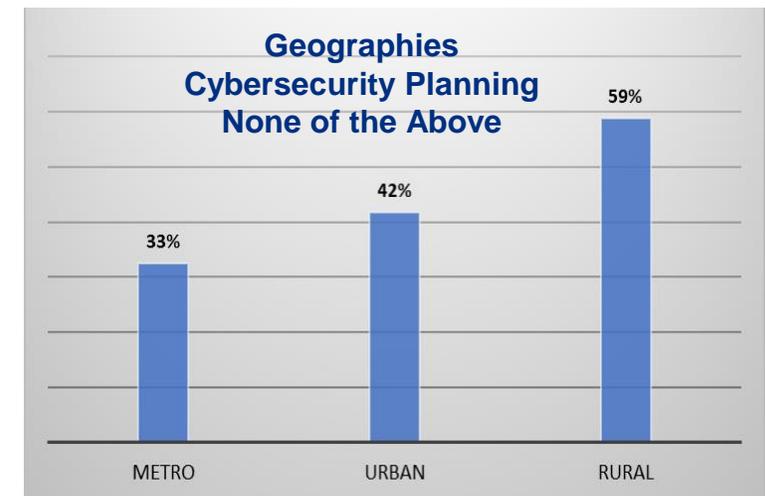
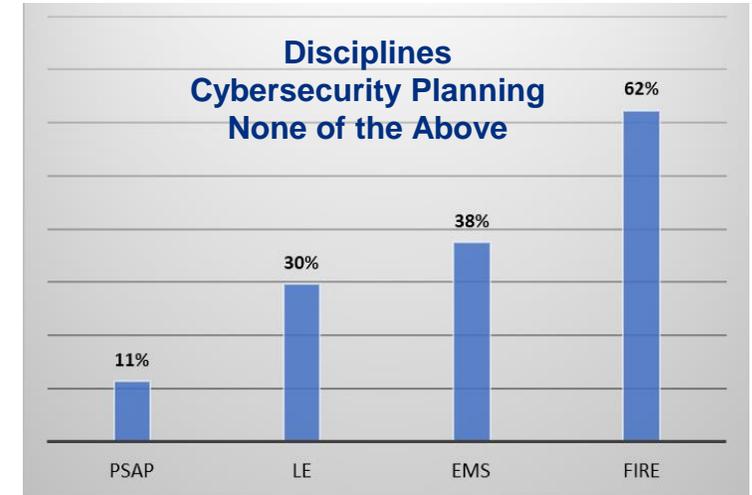


# SNS: Cybersecurity Planning

## Elements that Organizations Incorporate into Cybersecurity Planning



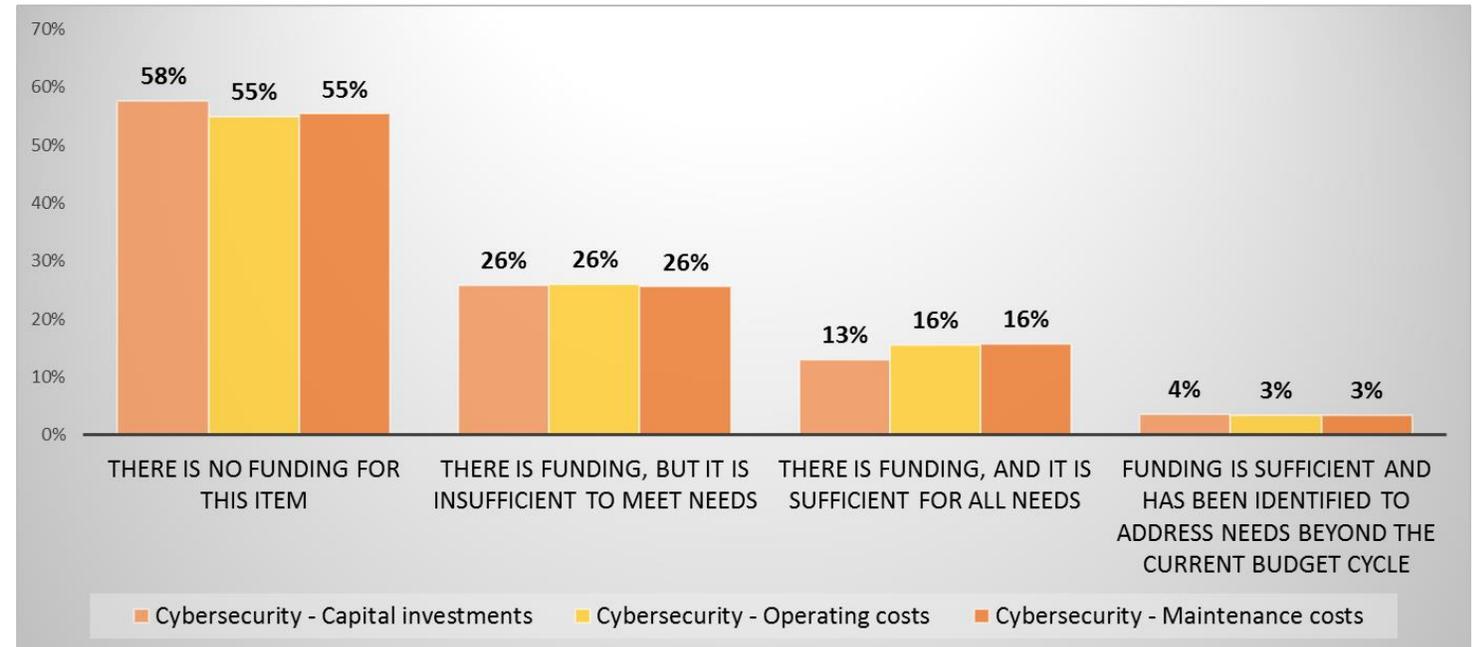
- 46% of organizations do not incorporate the listed cybersecurity measures into their cybersecurity planning
- 62% of fire departments indicated that they do not conduct any cybersecurity planning
- Almost 60% of public safety disciplines located in rural areas do not participate in cybersecurity planning



# SNS: Cybersecurity Funding

- Over 55% of organizations indicated that they don't have funding for cybersecurity capital investments or operating and maintenance costs
- Additionally, 26% of organizations indicated that their cybersecurity funding is insufficient to meet their needs

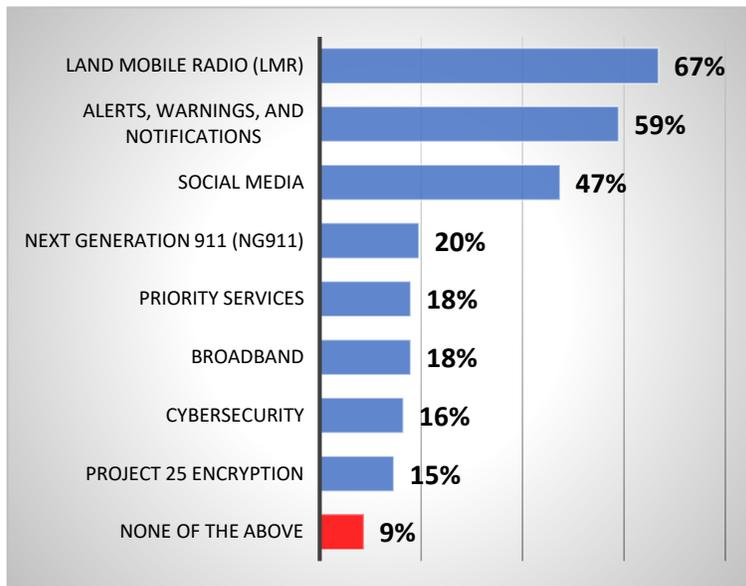
## Funding for Cybersecurity



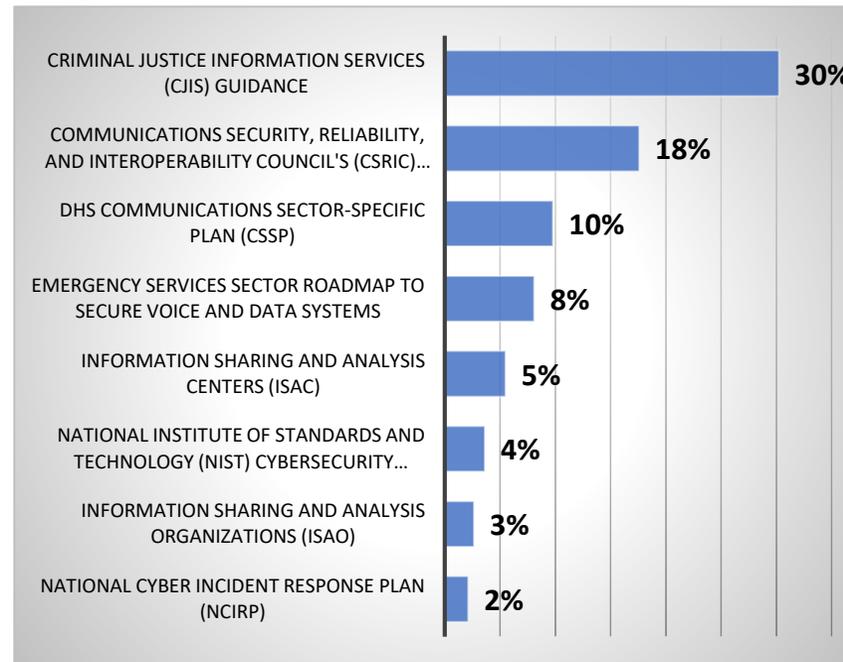
# SNS: Cybersecurity Additional Insights

- Organizations reported that cybersecurity is not prioritized as a topic for Standard Operating Procedures (SOPs) and is not included in Training and Exercise topics

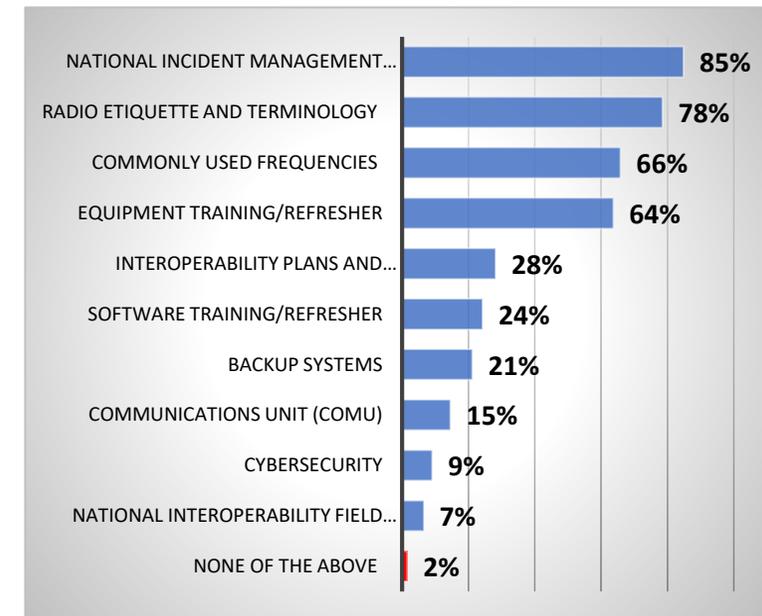
Topics Included in SOPs



Cybersecurity Guidelines and Standards Influencing SOPs



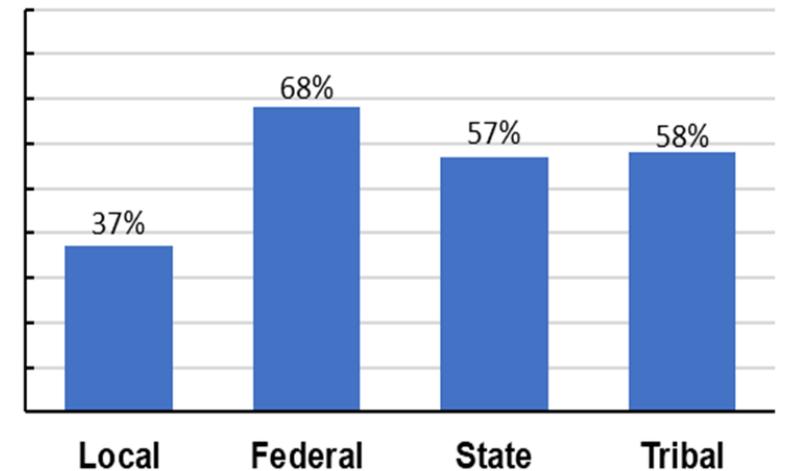
Topics Included in Emergency Communications Training



# NECP Success Indicators: Cybersecurity

- Implement the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework<sup>\[1\]</sup>](#)
- Perform a [Cyber Resilience Review](#)
- Include cybersecurity representatives in governance bodies
- Educate public safety agencies on cybersecurity risk mitigation
- Update training and exercise programs to address cybersecurity
- Develop and maintain a cyber incident response plan in coordination with the Statewide Interoperability Coordinator and information technology administrators

Percentage of Public Safety Organizations Whose Communications Have Been Impacted by Cybersecurity Breaches at Some Point in the Last 5 Years



# NIST Cybersecurity Framework July 2020

# Cybersecurity and the Economy

Security is about trust: can technology be used for its desired purpose without undue risk?



Without trust in the underlying technology,

Consumers will be reluctant to adopt new applications

Industry will be reluctant to invest in new infrastructure

Innovators will be reluctant to offer new ideas



As technology becomes further integrated into consumers lives ensuring that trust becomes more critical, and solutions need to be market-based to scale.

# Cybersecurity at NIST

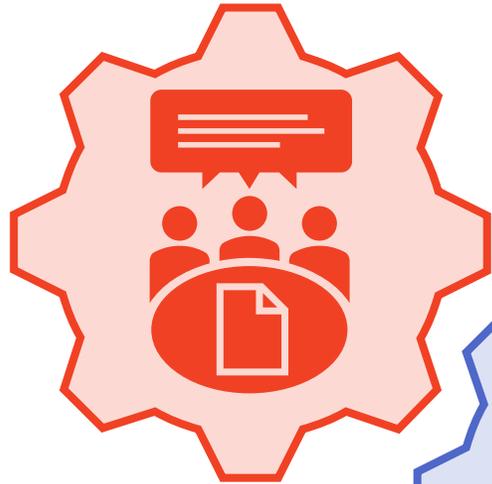
- Role in cybersecurity began in 1972 with the development of the Data Encryption Standard
- Using widely-accepted standards helps create competitive markets around market need through combinations of price, quality, performance, and value to consumers.
  - Ensure timely availability of standards, and associated testing,;
  - Achieve cost-efficient, timely and effective solutions to legitimate regulatory, procurement and policy objectives;
  - Promote standards and standardization systems that enable innovation and foster US competitiveness; and
  - Facilitate international trade and avoid the creation of unnecessary obstacles to trade.

# Cybersecurity Framework History

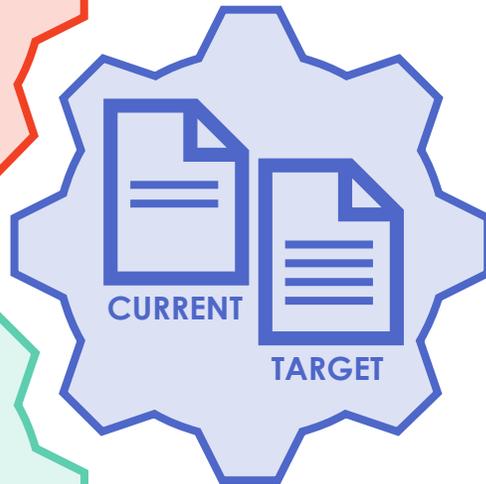
- February 2013 - Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*
- February 2014 – Version 1.0 of the Cybersecurity Framework released
- December 2014 - *Cybersecurity Enhancement Act of 2014 (P.L. 113-274)*
- May 2017 - Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- April 2018 – Version 1.1 of the Cybersecurity Framework released



# Cybersecurity Framework Structures



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy or cybersecurity risk, based on international standards



**Profiles** are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage cybersecurity risk



**Implementation Tiers** help an organization communicate about whether it has sufficient processes and resources in place to manage cybersecurity risk and achieve its Target Profile

# Key Framework Attributes

*Principles of Current and Future Versions of the Framework*

- Common and accessible language
- It's adaptable to many technologies, lifecycle phases, sectors and uses
- It's risk-based
- It's based on standards
- It's a living document
- Guided by many perspectives – private sector, academia, public sector



# An Excerpt from the Framework Core

Function	Category	Subcategory	Informative References
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	<b>PR.AC-6:</b> Identities are proofed and bound to credentials and asserted in interactions	<b>CIS CSC</b> , 16 <b>COBIT 5</b> DSS05.04, DSS05.05, DSS05.07, DSS06.03 <b>ISA 62443-2-1:2009</b> 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 <b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 <b>ISO/IEC 27001:2013</b> , A.7.1.1, A.9.2.1 <b>NIST SP 800-53 Rev. 4</b> AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		<b>PR.AC-7:</b> Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	<b>CIS CSC</b> 1, 12, 15, 16 <b>COBIT 5</b> DSS05.04, DSS05.10, DSS06.10 <b>ISA 62443-2-1:2009</b> 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
			<b>ISA 62443-3-3:2013</b> SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 <b>ISO/IEC 27001:2013</b> A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 <b>NIST SP 800-53 Rev. 4</b> AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions

23 Categories

108 Subcategories

6 Informative  
References

# Sample Resources

[www.nist.gov/cyberframework/framework-resources](http://www.nist.gov/cyberframework/framework-resources)



## Manufacturing Profile

[NIST Discrete Manufacturing Cybersecurity Framework Profile](#)

## Financial Services Profile

*Financial Services Sector Specific Cybersecurity “Profile”*

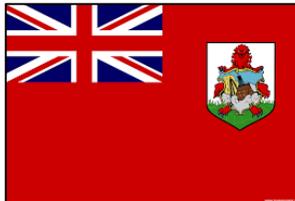
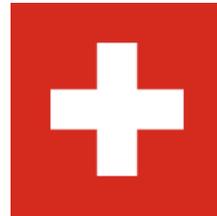
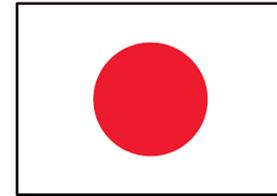
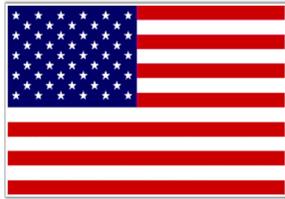


## Maritime Profile

[Bulk Liquid Transport Profile](#)

# International Use

*Some Translations and Adaptations World-Wide*



# Resources

## Website

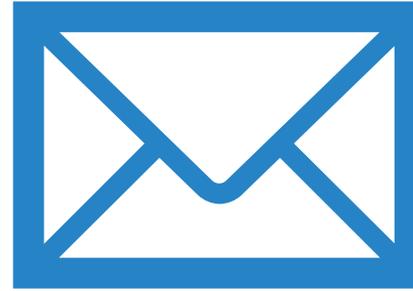
- <https://nist.gov/cyberframework>

## Contact

- [cyberframework@nist.gov](mailto:cyberframework@nist.gov)

## Stay Up to Date

- @NISTcyber



# Additional Resources

- [CISA Central](#)
- [CISA Cyber Resource Hub](#) and [CISA Alerts & Tips](#)
- [SAFECOM Nationwide Survey Results](#)
- [National Emergency Communications Plan](#)
- NIST Cybersecurity Framework ([NIST](#) and [CISA](#) resources)
- [DHS Cybersecurity Services Catalog for State, Local, Tribal, and Territorial Governments](#) [Note: Change to Tools Fact Sheet if published by then]
- [SAFECOM and National Council of Statewide Interoperability Coordinators Resources](#)
- [Emergency Communications Technical Assistance and Planning Guide](#)



# How You Can Take Action

- Take steps for your organization or jurisdiction to implement the NECP and achieve its success indicators
- Implement the NIST Cybersecurity Framework
- Download the [CRR Self-Assessment Package](#) or contact the [CISA Cybersecurity Advisor](#) to schedule an on-site visit to your organization



Questions?



# Upcoming Webinars

Join the Cybersecurity and Infrastructure Security Agency for webinars focused on:

## Implementing the National Emergency Communications Plan



**August 19<sup>th</sup>** – Make the most of your organization’s investments:  
Lifecycle Planning for Emergency Communications

**September 17<sup>th</sup>** – EXERCISE! EXERCISE! EXERCISE! Learn to turn  
evaluations into real-world communications improvements

All webinars start at 1pm ET

To join, use:

Webinar Link (for visual): <https://share.dhs.gov/necpwebinars>

Dial-In (for audio): 800-897-5813





**NECP Team**  
CISA Emergency Communications  
Email: [NECP@cisa.dhs.gov](mailto:NECP@cisa.dhs.gov)

