Workshop on Preventing and Recovering from Ransomware and Other Destructive Events

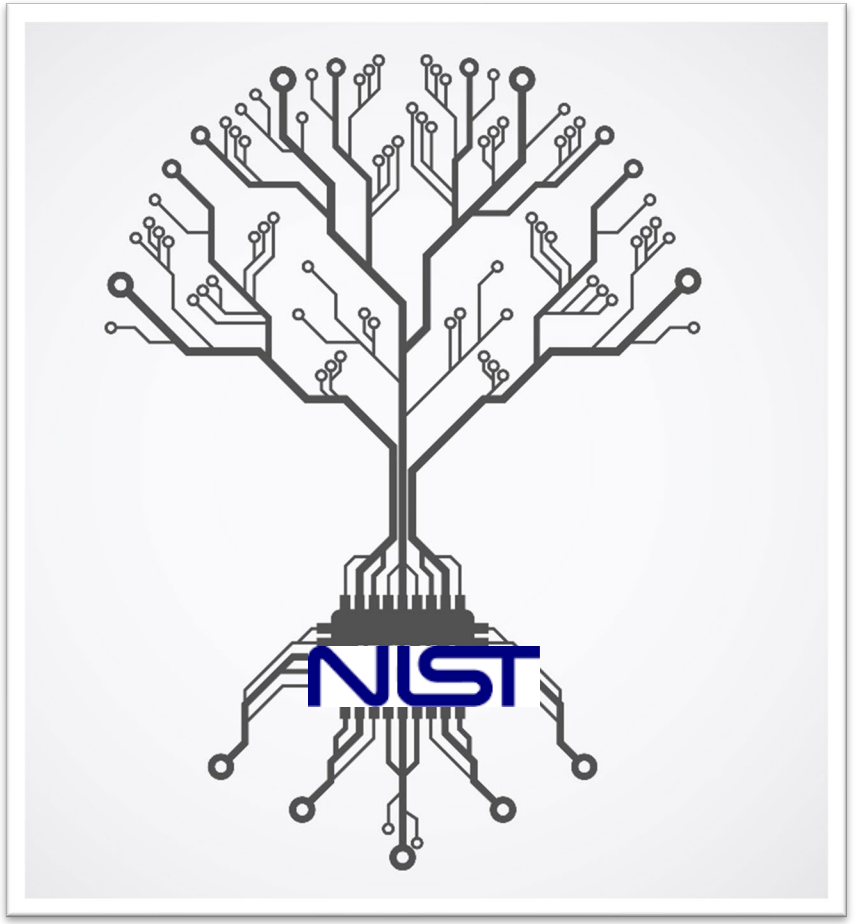
June 14, 2021

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

CULTIVATING TRUST

We cultivate trust in technology by advancing cybersecurity and privacy standards, technology, and measurement science.



NATIONAL CYBERSECURITY CENTER OF EXCELLENCE - WHO WE ARE

Accelerate adoption of secure technologies

collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

OUR GOALS

Provide practical solutions to address cybersecurity challenges

Increase adoption of cybersecurity

Accelerate innovation in secure technologies

OUR PRINCIPLES

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

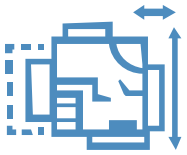
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide detailed guidance including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

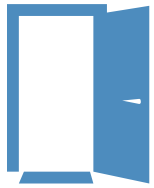
Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry



Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

WHY ARE WE HERE TODAY?

Purpose

- Help organizations mitigate, respond to, and recover from ransomware attacks

Objective

- Understand challenges to implementation, operations, and security associated with ransomware attacks
- Identify standards, guidelines, recommended practices, and use cases

Desired Outcomes

- Improve content and usability of existing NIST guidance addressing ransomware and data security
- Identify new areas of research and practical application
- Provide effective architectures, capabilities, and strategies for preventing and recovering from ransomware attacks
- Initiate development and demonstration of playbooks and other resources leveraging commercial technology and approaches

PRESENTERS AND ATTENDEES

- Subject matter experts and practitioners from government and industry

- Nearly 1,300 registrants
  - Government - Federal, State, and Local
  - Academia
  - Private Industry
  - Non-Profits/Not-for-Profits
  - Welcome to the Press!

TODAY'S AGENDA

11:00-11:05	**Welcome** – Kevin Stine, NIST Chief Cybersecurity Advisor
11:05-11:10	**Keynote** – Don Graves, Deputy Secretary, US Department of Commerce
11:10-11:25	**Workshop Overview and Background** – Kevin Stine
11:25-11:45	**Status of NIST Ransomware Activities** – Bill Fisher, NIST
11:45-11:55	**Moderated Q&A** – Mat Heyman, Impresa Management Solutions
11:55-12:00	**Break**
12:00-1:15	**Challenges Section** – Josh Corman, CISA; Phil Reiner, Institute for Security and Technology; Carmichael Patton, Microsoft; Sridhar Muppidi, IBM; Pranshu Bajpai, Motorola Solutions
1:15-1:25	**Moderated Q&A** – Bill Fisher, NIST
1:25-1:30	**Break**
1:30-2:10	**10-minute Lightning Talks** – Maria Vachino, Cyntegra; Travis Rosiek, BluVector; Guido Grillenmeier, Semperis; Brian Hymer, Quest; Temi Adebambo, AWS
2:10-2:20	**Moderated Q&A** – Karen Scarfone, Scarfone Cybersecurity
2:20-2:35	**Next Steps and Wrap-up** – Curt Barker, Dakota Consulting

ENGAGE WITH US!

- Questions to ransomware@nist.gov
- Provide **Comments** on NIST Publications
- Contribute through **Forums** and **Communities of Interest**
- Attend **Events**
- Conduct **Joint Research**
- Participate in **Standards Development**
- Follow us on **Social Media**

Credit: Shutterstock/Nazarkru

https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement