Resources for Ransomware Risk Management

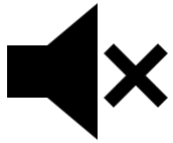
January 28, 2026

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

This webinar is being recorded

Notes and Reminders

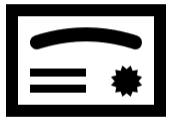
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar recording: This webinar will be recorded and posted here: nist.gov/itl/smallbusinesscyber/events Registrants will be notified via email when the recording is available.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



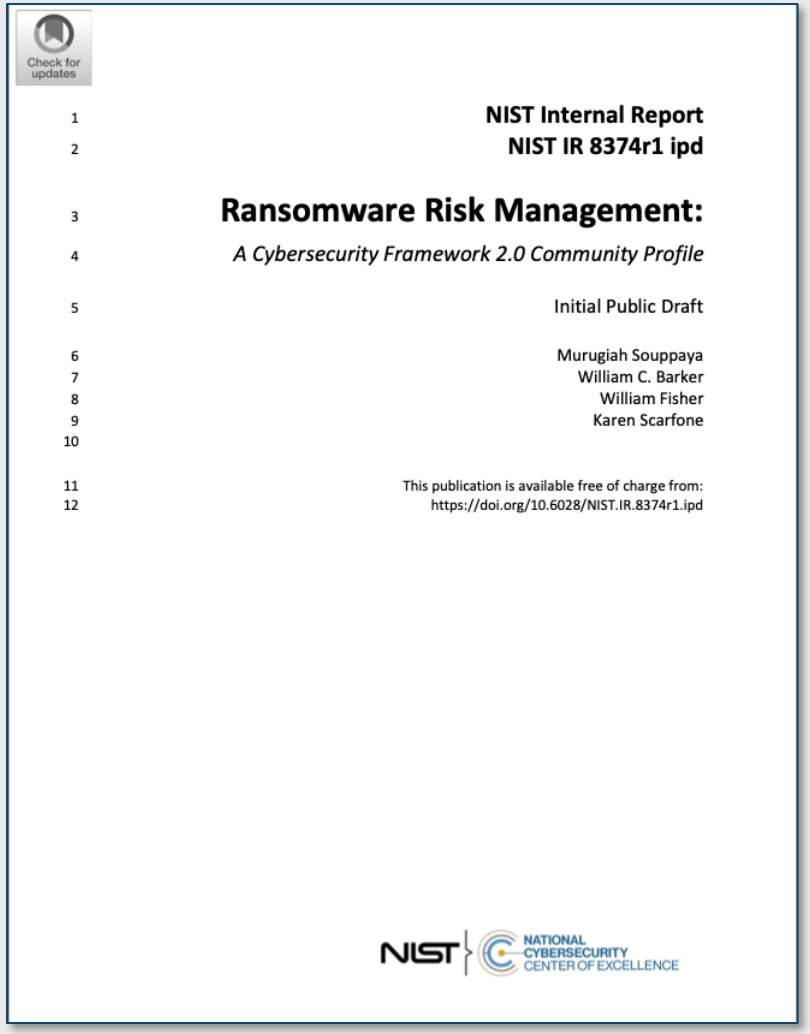
CEU/CPE credits: NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

Panelists:

- **Bill Fisher**, Security Engineer, NIST
- **Valecia Stocchetti**, Senior Cybersecurity Engineer, CIS Critical Security Controls, Center for Internet Security (CIS)
- **Michael Klein**, Senior Director for Preparedness and Response, Institute for Security and Technology (IST)
- **Daniel Eliot** (moderator), Lead for Small Business Engagement, Applied Cybersecurity Division, NIST

Note: There are no prepared slides for the panel discussion. You will see this slide for the duration of the panel.

New CSF 2.0 Profile – Ransomware Risk Management



Check for updates

NIST Internal Report
NIST IR 8374r1 ipd

Ransomware Risk Management:

A Cybersecurity Framework 2.0 Community Profile

Initial Public Draft

Murugiah Souppaya
William C. Barker
William Fisher
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374r1.ipd

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Document Updated to CSF 2.0
- Draft published in January 2025, final document soon to be published
- Document maps CSF categories and informative references (such as NIST SP 800-53) to ransomware risk activities
- Additional comments can be sent to ransomware@nist.gov
- https://csrc.nist.gov/pubs/ir/8374/r1/ipd

Center for Internet Security (CIS) Resources

- **Foundation**: CIS Controls and CIS Benchmarks
- Blueprint for Ransomware Defense (IST + CIS + Others)

  https://www.cisecurity.org/insights/blog/a-blueprint-for-ransomware-defense-using-the-cis-controls
- CIS Controls Cost of Cyber Defense: Implementation Group 1 (IG1)

  https://www.cisecurity.org/insights/white-papers/the-cost-of-cyber-defense-cis-controls-ig1
- CIS Community Defense Model (CDM)

  https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0
- CIS Controls Navigator (Mappings)

  https://www.cisecurity.org/controls/cis-controls-navigator
- CIS SecureSuite (Membership and Platform)

  https://www.cisecurity.org/cis-securesuite
- Multi-State Information Sharing and Analysis Center (MS-ISAC) Services

  https://www.cisecurity.org/ms-isac

Institute for Security and Technology Resources

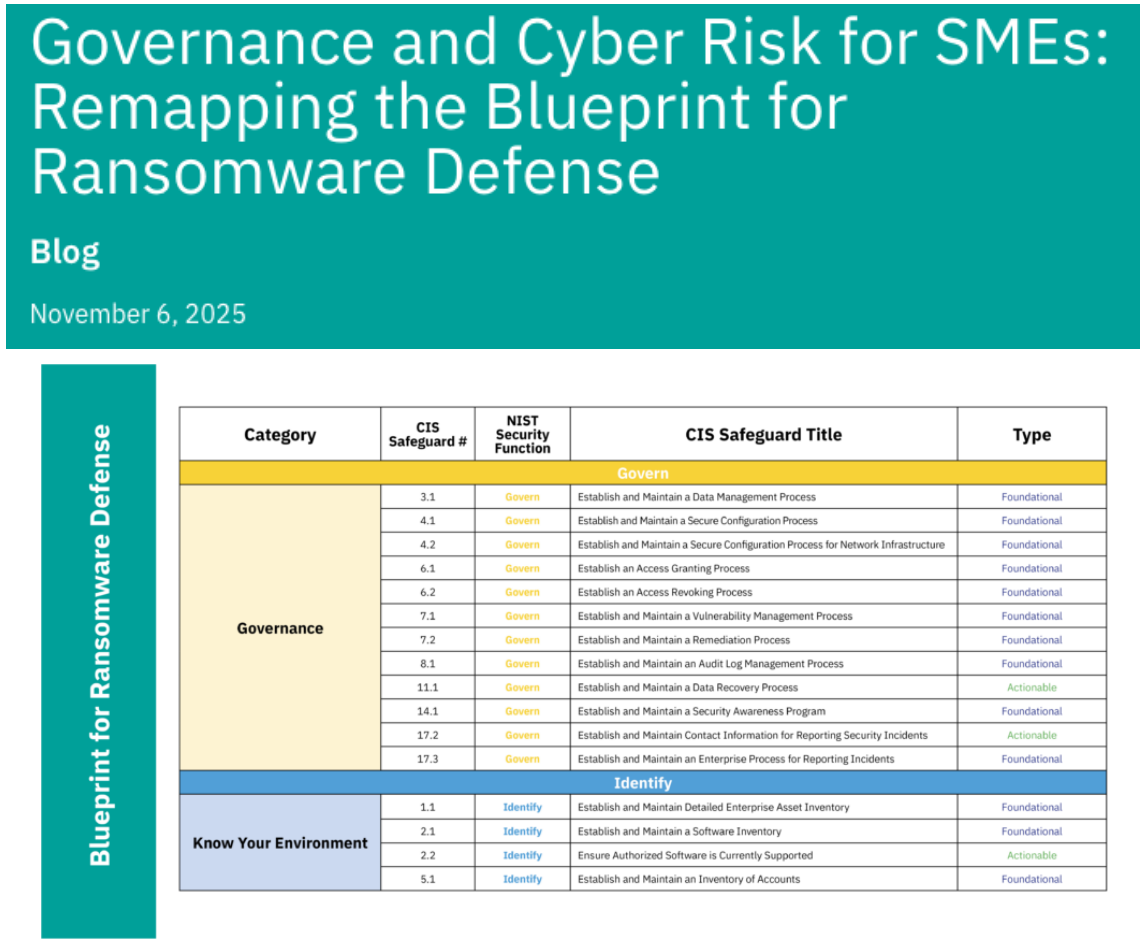
Blueprint Collaboration with CIS/NIST

Goal: Move from competing control sets to combined guidance focused on smallest SMEs (0-5 IT Staff)

- Remapped Blueprint to Align with CSF 2.0, including Govern
- Blog post with questions for small orgs to ask their MSP

Protecting Critical Infrastructure

- Schools: K-12 Cyber Defense Coalition
- Water & Hospitals: UnDisruptable27



Category	CIS Safeguard #	NIST Security Function	CIS Safeguard Title	Type
Govern				
Governance	3.1	Govern	Establish and Maintain a Data Management Process	Foundational
	4.1	Govern	Establish and Maintain a Secure Configuration Process	Foundational
	4.2	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Foundational
	6.1	Govern	Establish an Access Granting Process	Foundational
	6.2	Govern	Establish an Access Revoking Process	Foundational
	7.1	Govern	Establish and Maintain a Vulnerability Management Process	Foundational
	7.2	Govern	Establish and Maintain a Remediation Process	Foundational
	8.1	Govern	Establish and Maintain an Audit Log Management Process	Foundational
	11.1	Govern	Establish and Maintain a Data Recovery Process	Actionable
	14.1	Govern	Establish and Maintain a Security Awareness Program	Foundational
	17.2	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	Actionable
	17.3	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	Foundational
Identify				
Know Your Environment	1.1	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Foundational
	2.1	Identify	Establish and Maintain a Software Inventory	Foundational
	2.2	Identify	Ensure Authorized Software is Currently Supported	Actionable
	5.1	Identify	Establish and Maintain an Inventory of Accounts	Foundational

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Questions?