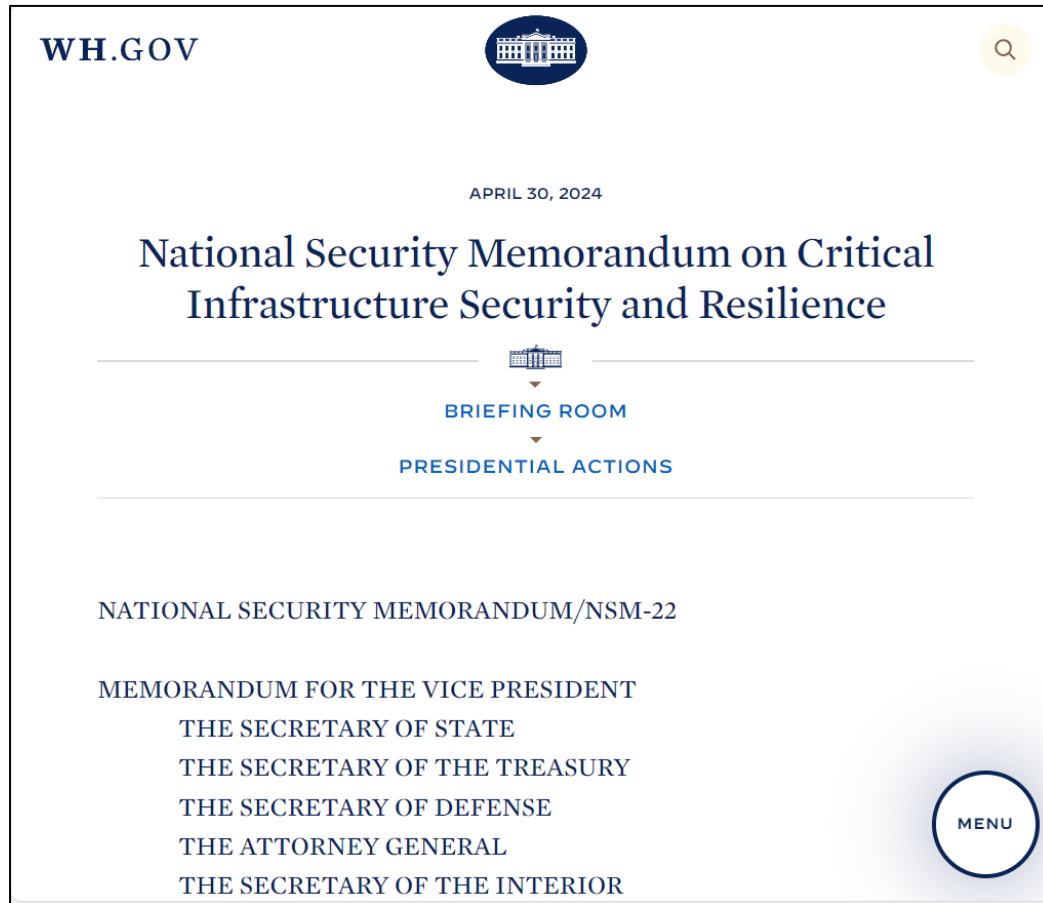


COORDINATION ON CRITICAL INFRASTRUCTURE PROTECTION AT THE U.S. TREASURY

Laura Bate - Acting Deputy Director, Cyber Intelligence and Risk Analysis,
Office of Cybersecurity and Critical Infrastructure Protection,
U.S. Department of the Treasury

National Security Memorandum on Critical Infrastructure (NSM – 22)



WH.GOV

APRIL 30, 2024

National Security Memorandum on Critical Infrastructure Security and Resilience

BRIEFING ROOM

PRESIDENTIAL ACTIONS

NATIONAL SECURITY MEMORANDUM/NSM-22

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR

MENU

- Issued April 30, 2024
- Replaces PPD-21 from February 2013
- Publicly Available:
<https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>

National Security Memorandum on Critical Infrastructure (NSM-22)

National Security Memorandum - 22 coordinates a complex system:

- 16 sectors
- Mostly privately-owned infrastructure
- Many stakeholders:
 - Regulators
 - State, local, tribal, and territorial governments
 - Private industry



[Chemical Sector](#)



[Commercial Facilities Sector](#)



[Communications Sector](#)



[Critical Manufacturing Sector](#)



[Dams Sector](#)



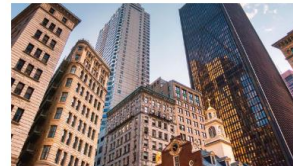
[Defense Industrial Base Sector](#)



[Emergency Services Sector](#)



[Energy Sector](#)



[Financial Services Sector](#)



[Food and Agriculture Sector](#)



[Government Services and Facilities Sector](#)



[Healthcare and Public Health Sector](#)



[Information Technology Sector](#)



[Nuclear Reactors, Materials, and Waste](#)



[Transportation Systems Sector](#)



[Water and Wastewater Systems](#)

National Security Memorandum on Critical Infrastructure (NSM-22)

National Security Memorandum – 22 (NSM-22) responds to a changing world:

- Technological advances
 - Cloud
 - AI
 - Quantum
- Threat actors (e.g. Volt Typhoon)
- Non-cyber risks



National Security Memorandum on Critical Infrastructure (NSM – 22)

Major functions of NSM – 22 include:

- Centralizing the role of the National Coordinator and requiring a biennial National Risk Management Plan,
- Expanding intelligence sharing,
- Elevating the importance of minimum security and resilience requirements, and
- Clarifying the role of Sector Risk Management Agencies (SRMAs).

The screenshot shows the top portion of a document from WH.GOV, dated APRIL 30, 2024. The title is "National Security Memorandum on Critical Infrastructure Security and Resilience". Below the title are navigation links for "BRIEFING ROOM" and "PRESIDENTIAL ACTIONS". The document is identified as "NATIONAL SECURITY MEMORANDUM/NSM-22" and is addressed to "MEMORANDUM FOR THE VICE PRESIDENT" and "THE SECRETARY OF STATE". Other recipients listed are "THE SECRETARY OF THE TREASURY", "THE SECRETARY OF DEFENSE", "THE ATTORNEY GENERAL", and "THE SECRETARY OF THE INTERIOR". A search icon is in the top right, and a "MENU" button is in the bottom right.

NSM-22: Strategic Guidance and National Priorities for U.S. Critical Infrastructure

Priority Risk Areas:

- Address cyber and other threats posed by the People's Republic of China (PRC).
- Manage the evolving risks and opportunities presented by Artificial Intelligence (AI) and other emerging technologies.
- Identify and mitigate supply chain vulnerabilities.
- Incorporate climate risks into sector resilience efforts.
- Address growing dependency of critical infrastructure on space systems and assets.

Priority Risk Mitigations:

- Build resilience to withstand and recover rapidly from all threats and hazards.
- Adopt security and resilience baseline requirements.
- Incentivize service providers to drive down risk at scale.
- Identify areas of concentrated risk and systemically important entities

Office of Cybersecurity and Critical Infrastructure Protection Overview

OCCIP's mission is to improve the security and resiliency of the financial services sector through Treasury's unique role in the Financial and Banking Information Infrastructure Committee (FBIIIC) and the Group of Seven, both as a cabinet-level Department, and as sector risk management agency for the financial services sector.

OCCIP Activities:

- Central information node
- Resilience Exercises
- Coordinate incident response
- Policy coordination for cybersecurity and critical infrastructure protection

International Policy

- G7 CEG
 - Co-Chair of G7 Cyber Expert Group
 - Cloud Usage and Security and Emerging Technology workstreams
- Bilateral Engagements
 - OCCIP maintains bilateral relationships with several international financial authorities, this includes joint exercises, cyber threat information sharing, incident response playbooks, study visits, and project-based work
- Other Activities
 - Financial Stability Board (Format for Incident Reporting Exchange)
 - Capacity building and partnership activities

Domestic Cyber Policy

- **FBIIC:** OCCIP Chairs the Financial and Banking Information Infrastructure Committee (FBIIC), which facilitates coordination and communication among 18 financial regulators, enhancing the resiliency of the financial sector and promoting public-private partnership.
- **FSSCC:** OCCIP interfaces with the Financial Services Sector Coordinating Council which is composed of 70+ members, including trade associations, financial market utilities, banks, insurers, and other financial sector firms.
- **Cloud Executive Steering Group (CESG):** Public-private partnership consisting of agency heads and sector CEOs from the FBIIC and FSSCC dedicated to bolstering regulatory and private sector cooperation. CESG has recently published a series of documents intended to equip financial institutions with effective practices for secure cloud adoption.
- **Project Fortress:** Treasury established Project Fortress to improve the security and resilience of the financial services sector through forward-leaning public-private information sharing mechanisms that will benefit financial institutions of all sizes, leveraging a combination of data sources, threat feeds, and collaboration spaces to improve information flows to the private sector.

Sector Cyber Resilience

- **Incident Management:** Focuses on coordinating the incident management process for the FBIIC and Treasury's response to incidents impacting the financial sector's ability to conduct operations.
- **Operational Risk:** Conducts sector-focused work with financial industry and regulatory partners to develop a financial sector risk model design to identify key risk areas for the financial services sector to help inform and prioritize OCCIP's SRMA function.
- **Exercise Management:** Works with private and public partners to conduct various exercises that raise awareness of incident management best practices, test the effectiveness of policies and procedures, identify gaps in preparedness, and recommend areas for future sector collaboration.
- **Incident Reporting:** OCCIP has been monitoring the progress of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) and working with the Cybersecurity and Infrastructure Security Agency (CISA) to stay up to date on incident response and management impacts to the financial sector.

Cyber Intelligence and Risk Analysis

- **Written Products:** Circulars, Indicator Notices, Spotlight reports, threat trends, and other information is gathered, analyzed, and relayed as widely as possible via email to U.S. Government partners and the private sector.
- **Unclassified Threat Exchange:** Invited subject matter experts present cutting-edge threat information each month to an audience of practitioners from U.S. financial institutions. The events regularly draw hundreds of viewers and encourage audience questions.
- **Private Sector Clearance Program:** In partnership with the U.S. Department of Homeland Security, OCCIP nominates private sector partners with a need to know for security clearances, allowing for more detailed conversations on emerging threats to the sector.
- **Financial Services Explained Day:** Alongside private sector counterparts, OCCIP hosts an annual information session to help colleagues in intelligence, law enforcement, cybersecurity, and other elements of government to better understand the financial services sector and its informational requirements.

QUESTIONS?



OCCIP

Office Of Cybersecurity
& Critical Infrastructure
Protection