Congressional Research Service
Informing the legislative debate since 1914

HSA@20 Episode Companion: Cybersecurity

April 10, 2023

This Insight accompanies the "Cybersecurity" episode of *The Homeland Security Act at 20* podcast series and includes background information on the issues discussed during the podcast.

Cybersecurity and the Homeland Security Act (HSA)

Although the Homeland Security Act of 2002 (HSA; P.L. 107-296) rearranged some cybersecurity functions, substantive changes to cybersecurity began in earnest 2013.

Phase I: Before 9/11

- Cybersecurity was on the agenda, but not in the forefront of public debate.
  - Road Map for National Security: Imperative for Change: The Phase III Report of the U.S. Commission on National Security/21st Century, informally known as the Hart-Rudman Report.
  - Senator Domenici's bill: S.1407, the Critical Infrastructures Protection Act of 2001.
- "Information security" policy development and operations were largely being conducted by the Department of Defense in the classified realm, as they had the capability, the expertise, the capacity, and the authority to carry it out.
  - Other federal actors included
    - The National Institute of Standards and Technology (NIST)—the long-standing federal authority for computer security; and
    - Law enforcement agencies, such as the Federal Bureau of Investigation (FBI) and U.S. Secret Service (USSS).

Phase II: The HSA Moves Some Elements to DHS; Policy Doesn't Change Much

- The HSA moved certain components into the Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection Directorate (IAIP) in 2003:
  - The Federal Computer Incident Response Center from the General Services Administration (now the U.S. Computer Emergency Response Team (US-CERT));
  - The National Communications System from the Department of Defense;

CRS INSIGHT
Prepared for Members and
Committees of Congress

  - The National Infrastructure Protection Center from the FBI; and
  - The Energy Security and Assurance Program from the Department of Energy.
- Policymaking was characterized by the initial development of coordination mechanisms and federal strategies.
  - Cybersecurity was (and still is) seen as a shared responsibility.
  - DHS's cybersecurity activity focused on existing communication and coordination roles, rather than establishing new ones.
- The first U.S. national cybersecurity strategy was the George W. Bush Administration's National Strategy to Secure Cyberspace (February 2003).
- The HSA's original cybersecurity provisions are at P.L. 107-296, Title II, Subtitle C, "Information Security."
- USSS authorities for investigating unauthorized access to computers and access device fraud (18 U.S.C. §1029(d)) come from the Comprehensive Crime Control Act of 1984 (P.L. 98-473).
- **Further cybersecurity reorganization in the early years of DHS:**
  - IAIP dissolved in a July 2005 reorganization, and many of these functions moved to the Directorate for Preparedness.
  - In 2007, the Post Katrina Emergency Management Reform Act (P.L. 109-295, Title VI) removed part of the Directorate, returning it to FEMA.
  - A further reorganization created the National Protection and Programs Directorate (NPPD), which included the cybersecurity functions.

Phase III: Congress Establishes New Federal Roles and Resources

- "Catalytic" cybersecurity events:
  - Heartland Payment Processing data breach (a.k.a. the "Target breach"): Senate Committee on Commerce, Science, and Transportation March 26, 2014 hearing, "Protecting Personal Consumer Information From Cyber Attacks and Data Breaches."
  - North Korean cyber operations: DPRK Cyber Threat Advisory (cisa.gov).
- **Selected evolutionary legislative steps on cybersecurity:**
  - **113th Congress:**
    - P.L. 113-282, the "National Cybersecurity Protection Act of 2014"—National Cybersecurity and Communications Integration Center (NCCIC) authorization in NPPD;
    - P.L. 113-274, the "Cybersecurity Enhancement Act of 2014"—NIST Cybersecurity Framework; and
    - P.L. 113-283, the "Federal Information Security Modernization Act of 2014"—first comprehensive ".gov" cybersecurity reform since 2002.
  - **114th Congress:** P.L. 114-113, Division N, the "Cybersecurity Act of 2015"—created new information sharing programs at NPPD that operate outside the federal government.
  - **115th Congress:** P.L. 115-454, the "Cybersecurity and Infrastructure Security Agency Act of 2018"—CISA Authorization.

- **116th Congress:** P.L. 116-283, the "William H. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021"—National Cybersecurity Director authorized (Title XVII, §1752), implementing a key recommendation from the Cyberspace Solarium Commission.
- **117th Congress:**
    - Two supplemental appropriations measures included authorization and funding for new initiatives:
        - American Rescue Plan Act (ARPA; P.L. 117-2)—included $2 billion for federal IT improvements, including $650 million for CISA for cybersecurity risk mitigation.
        - Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58)—included $2 billion for cybersecurity modernization and resiliency improvements, including
            - $20 million each year from FY2022-FY2026 for the "Cybersecurity Response and Recovery Fund";
            - $1 billion for FEMA grants spread over FY2022-FY2025 for state, local, tribal and territorial governments to improve cybersecurity and critical infrastructure protection;
            - $250 million for energy sector cybersecurity research and development; and
            - $250 million to fund the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program.
    - The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Division Y of P.L. 117-103; CIRCIA) directs CISA to issue a regulation requiring covered private sector entities to report to the federal government when they experience certain cyber incidents.

Why Total Federal Cybersecurity Spending Cannot Be Tracked

- Methodologies that assess what does and does not count as "cybersecurity" evolve over time.
- Not all appropriations specify amounts for cybsersecurity spending.
- Cross-cutting discussion of federal cybersecurity funding is provided in the Analytical Perspectives volume of the President's annual budget request.
- This is primarily an analysis of the funding requested, rather than the funding provided, or how prior year appropriations were applied to cybersecurity or information technology.
- An authoritative top-line total or historical tracking would not be indicative of whether the federal government is investing its resources in the right places.

Looking Ahead

- Congress has recently taken an interest in the interaction and relationship between the public and private sectors for cybersecurity.
- The *National Cybersecurity Strategy* released in March 2023, provides Congress a an additional opportunity to focus oversight on the agency activities outlined in the strategy and debate legislative options concerning shifts in responsibilities and regulatory changes.

FOR MORE INFORMATION

- For more information on cybersecurity issues, see CRS Video WVB00451, *2022 Issues & Policy - The Evolution of Cybersecurity Issues in the 117th Congress*, by Chris Jaikaran.
- For more episodes of this podcast series, search "HSA@20" on the CRS website.

NEXT EPISODE

HSA@20: Immigration.

Music: Icas, by Audiorezout, as carried on freemusicarchive.org, under the terms of its Creative Commons Attribution-NonCommercial 4.0 International license.

Author Information

William L. Painter, Coordinator
Specialist in Homeland Security and Appropriations

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.