Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

March 16, 2022

Critical Infrastructure Security and Resilience: Countering Russian and Other Nation-State Cyber Threats

The United States and its allies have levied economic sanctions against Russia following its invasion of Ukraine. Many observers fear Russian state or state-sponsored cyberattacks against U.S. critical infrastructure in response. Critical infrastructure is defined in statute as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Department of Homeland Security (DHS) is the lead federal agency for critical infrastructure security and resilience (CISR).

The DHS Cybersecurity and Infrastructure Security Agency (CISA) has issued numerous alerts and other warnings to private-sector companies about malicious cyber activities by Russian state or state-sponsored actors that may harm critical infrastructure. According to the CISA alert revised on March 1, 2022, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to Critical Infrastructure*, "Russian state-sponsored ... actors have used sophisticated cyber capabilities to target a variety of U.S. and international critical infrastructure organizations." The alert identified the energy, healthcare, and communications systems and assets as frequent targets.

This In Focus provides an overview of the U.S. critical infrastructure community, describing the current development of cyber risk management programs and activities in the Energy, Healthcare and Public Health (HPH), and Communications sectors. In recent decades, the federal government has supported voluntary programs and activities intended to develop common perspective, risk awareness, and risk management culture within a diverse and evolving community of critical infrastructure stakeholders. During this time, development of CISR-oriented communities of interest defined by robust sector and cross-sector professional networks, multilateral flows of critical infrastructure information, collaboration with relevant government agencies, and investments in resilience has been uneven.

The Critical Infrastructure Community

CISA commonly describes its partners in the national CISR enterprise as the critical infrastructure community. This community—more concept than organization—is the aggregate of people and organizations engaged in security and resilience activities related to critical infrastructure. It includes thousands of private-sector businesses and enterprises, nonprofits, researchers, analysts, and technologists, as well as interested legislators, government officials, and law enforcement and emergency management personnel.

At the federal level, the critical infrastructure community is organized under auspices of presidential policy directives, which assign DHS (acting through CISA) responsibility for leadership and interagency coordination of voluntary public-private partnerships across 16 designated critical infrastructure sectors and numerous subsectors. DHS delegates this responsibility to other agencies in some cases. The responsible agency in each sector is referred to as the Sector Risk Management Agency (SRMA).

Because much of the nation's critical infrastructure is owned and operated by the private sector, implementation of federal cybersecurity initiatives to counter nation-state and other threats often depends upon the willingness and ability of private-sector entities to engage with CISR-oriented communities of interest, to make relevant resilience investments, and to report cyber incidents quickly—even those that may pose reputational, legal, or regulatory consequences. Likewise, owner-operators of vulnerable systems may have to absorb significant up-front business costs to increase security. Owner-operators of systems that do not meet the statutory definition of critical infrastructure may still suffer from attacks that present systemic risk, given the interconnectedness of such systems.

Energy Sector

The Energy Sector consists of two subsectors—electricity, and oil and natural gas. The Department of Energy (DOE) is the designated SRMA.

Electricity

The North American Electric Reliability Corporation (NERC)—a federally authorized, industry-led reliability organization—develops and enforces mandatory reliability standards that address cybersecurity and other risks affecting the nation's bulk power system. NERC plays a significant role in voluntary best practices and information-sharing programs. NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which facilitates sharing of cyber threat information and analysis between industry partners and government through alerts, exercises, and other means. ISACs in other sectors have similar functions. E-ISAC manages a DOE program for real time cyber threat information sharing to protect critical infrastructure.

According to DOE, utilities participating in its information-sharing program provide power to over 75% of customers in the continental United States. NERC periodically organizes grid security exercises. A major November 2021 exercise included 700 participants from the bulk power industry, according to media reports. Prior to the 2021

exercise, some observers voiced concerns about regulatory gaps and inadequate standards. NERC reliability standards are consensus-based, and mostly apply to larger utilities engaged in interstate transmission.

Oil and Natural Gas

There is no industry reliability organization analogous to NERC in any oil and gas industry segment. Standards development functions are led by major industry trade groups on a largely voluntary basis. Certain voluntary consensus standards have been incorporated by reference into the Code of Federal Regulations, giving them legal effect. These standards are concentrated in the heavily regulated offshore segment and the pipelines subsector. Further—with the exception of pipelines—these standards focus on risks inherent to the physical operation of industrial equipment, rather than cybersecurity.

Industry groups own and operate the Oil and Natural Gas (ONG) ISAC. Some independent reports indicate slow progress in developing cybersecurity culture and meaningful community engagement. A 2020 report by the Lawrence Livermore National Laboratory on cybersecurity in the oil and gas subsector noted widespread deficiencies, including use of legacy assets lacking cybersecurity features, use of consumer-grade operating systems and software with known vulnerabilities, and a culture of general apathy in many enterprises. Industry groups assert they work closely with federal agencies to ensure "collaboration and communication at every point."

Healthcare and Public Health Sector

The HPH Sector includes both private-sector and public-sector entities for patient care, medical research and development (R&D), pharmaceutical production, insurance, and other purposes. Malicious cyber actors—sometimes with nation-state sponsorship or acquiescence—have increasingly targeted the HPH Sector to acquire healthcare technology R&D, medical information, and patient data. Disruption of public health functions may be an end in itself in some cases.

The Department of Health and Human Services (HHS) is the designated SRMA. Limited HHS regulatory authorities and programs focus on maintaining privacy of patient health information and the operational integrity of agency computer systems.

HHS's private-sector counterpart, the HPH Sector Coordinating Council (SCC), has created several relevant industry working groups in recent years to increase threat reporting and analysis, information sharing, and adoption of best practices. The Cybersecurity Working Group reports increasing stakeholder engagement. In addition, the Health-ISAC has operated since 2010 and remains active.

A 2018 survey of 600 healthcare organizations on industry adoption of cybersecurity best practices showed that most organizations participate in one or more cybersecurity information-sharing and analysis organizations. Indicators of substantive private-sector engagement with such organizations and adoption of best practices were more mixed.

Communications Sector

The communications sector includes five segments: broadcasting, cable, satellite, wireless, and wireline. DHS is the designated SRMA. It operates the National Coordination Center, which hosts the Communications ISAC and provides operational support for specific national-level incidents. DHS and other agencies do not regulate cybersecurity risk management activities of private-sector partners.

DHS's private-sector counterpart, the Communications SCC (CSCC), supports numerous public-private partnership activities for threat reporting and analysis, information sharing, and adoption of best practices. In letters and filings to federal agencies, the CSCC has noted persistent information-sharing obstacles related to security classification and legal exposure. The CSCC has also noted limited community-wide awareness of collaboration and information-sharing channels, and insufficient grant funding for cybersecurity resilience activities.

Cross-Sector Issues

Many community members identify information sharing, government outreach to the private sector, and return on investment for public-private collaborations as areas for improvement. A CISA program implemented under the Cybersecurity Information Sharing Act of 2015 to increase public-private sharing of cyber threat indicators and defensive measures via automated means elicited only sparse participation, according to a 2019 interagency report to Congress. CISA stated it was implementing changes.

A DHS after-action report on its Cyber Storm 2020 exercise noted that some private-sector participants bypassed established information-sharing channels, and were therefore less effective in responding to the simulated nation-state attack. The report called for DHS to increase outreach and clarify coordination pathways for private-sector partners. It also called upon private-sector partners to share more information to help identify coordinated cyberattacks.

A 2021 Belfer Center study of cybersecurity collaboration between critical infrastructure owner-operators and government reported that established information channels were often left unused. "Many private-sector companies don't often see the government as a useful partner and decline to work with them if they don't have to," it said.

Recent Legislation

In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 as part of the Consolidated Appropriations Act, 2022 (H.R. 2471), which was signed by the President on March 15, 2022. It requires covered critical infrastructure entities to report certain breaches and ransom payments to CISA, among other provisions. Also see CRS Report R46944, *Cybersecurity: Comparison of Selected Cyber Incident Reporting Bills—In Brief*, by Chris Jaikaran.

Brian E. Humphreys, Analyst in Science and Technology Policy

Disclaimer