National Cybersecurity FFRDC

Under the sponsorship of the U.S. Commerce Department’s National Institute of Standards and Technology, MITRE operates the National Cybersecurity FFRDC to enhance cybersecurity and protect national information systems.

Who We Are

In October 2014, the National Institute of Standards and Technology (NIST) selected MITRE to operate the nation’s first FFRDC solely dedicated to cybersecurity. The FFRDC supports the National Cybersecurity Center of Excellence’s (NCCoE’s) goal of accelerating the adoption of secure technologies to address today’s most pressing cybersecurity challenges.

Working with NIST, the FFRDC will help businesses secure their critical data and infrastructures by fostering public–private collaborations to identify and solve today’s real-world cybersecurity threats. Together, they will offer pragmatic approaches based on commercially available technologies.

NCCoE uses an innovative collaboration model to draw on a wide range of expertise. The team includes researchers from the University of Maryland, College Park, and the University of Maryland, Baltimore County. It also includes support from universities on the Academic Affiliates Council and key stakeholders from industry and government.

Providing Real-World Cybersecurity Best Practices

The NCCoE was originally established in 2012 by NIST, the State of Maryland, and Montgomery County, Md. to engage public and private partners in long- and short-term collaboration efforts. The center works with members of industry sectors—such as healthcare, financial services, and energy—to identify shared concerns, develop model cybersecurity designs, and publish practice guides. It also works with small groups of vendors to develop “building blocks,” which address technical cybersecurity challenges common across multiple industries.

Cybersecurity is a core capability at MITRE. Over the course of more than 40 years of working with federal agencies to secure the nation’s critical cyber infrastructure, we have the necessary experience to draw on to help NCCoE advance the state of cybersecurity practice. MITRE’s ongoing collaborations with the cybersecurity community, particularly in advancing standards and facilitating threat-sharing, will also complement the NCCoE’s mission.
The FFRDCs that MITRE operates take on tough technical challenges of national importance and provide leading-edge, practical, and cost-effective solutions. Here are some examples of recent MITRE achievements.

Creating a Uniform Approach to Cybersecurity

Combining technical expertise with a cross-agency perspective, a MITRE team helped NIST develop the uniform cybersecurity guidelines and policies that are now used throughout the federal government. Adopted by the Joint Task Force Transformation Initiative (representing NIST, DoD, and the Office of the Director of National Intelligence) in 2013, these security controls dramatically altered how government engages in cybersecurity. Where different agencies once followed different policies, they now embrace a common approach. This uniformity has improved efficiency, fostered reciprocity, reduced costs, and strengthened defense capabilities—having a far-reaching impact on the economic and security interests of the nation.

Forging Partnerships to Share Threat Information

Today’s cyber threat is too complex and sophisticated for any one company, organization, or government agency to battle alone. MITRE has helped pioneer a model for cyber defense that is based on teamwork. In 2011, we helped launch the Advanced Cyber Security Center, the first consortium in New England that brings together diverse public and private entities to combat cyber threats. ACSC members share detailed threat information that could help in preventing, detecting, and responding to cyber attacks. MITRE is now helping develop similar threat-sharing consortiums elsewhere in the country, such as the Western Cyber Exchange in Colorado.

At the Forefront of Software Standards Efforts

For decades, MITRE has been at the forefront of major software standards efforts to promote meaningful and accurate information exchange and improve security for the nation’s infrastructure. One early effort was the Common Vulnerabilities and Exposures List (CVE), launched in 1999 to offer a consistent way to catalog specific software vulnerabilities. Currently sponsored by the Department of Homeland Security, over the years CVE has received funding and sponsorship from a host of federal agencies, including the IRS, the Defense Information Systems Agency, NASA, the Air Force, and NIST. MITRE launched the Common Weakness Enumeration registry (CWE) in 2005 to identify general security issues that could affect any software product. We helped compile the 2011 list of the Top 25 Most Dangerous Software Errors to help programmers avoid costly and dangerous mistakes.