PRACTICAL SOLUTIONS TO SECURE CYBER SYSTEMS

Artificial intelligence, the Internet of Things, 5G networks, satellite communications, and commercial space travel. Transformational technologies drive performance and efficiency in our work, processes, and lives. But even the smallest tweak has the potential to create vulnerabilities in cyber systems.

That's where MITRE's National Cybersecurity Federally Funded Research and Development Center (NCF) fills a critical need, scanning the continually shifting digital landscape for emerging, unexpected problems. Through NCF, MITRE's multidisciplinary teams research and analyze critical infrastructures and the complex ecosystems they support. With that information, we develop detailed guidance and actionable playbooks that stakeholders can use to mitigate cybersecurity vulnerabilities.

With funding from the National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence, NCF is the country's only federally funded research and development center dedicated solely to cybersecurity and developing standards to secure technology.

MITRE

> "NCF is a hub for continuous, collaborative innovation to meet our toughest cybersecurity challenges."
>
> Brian Abe, Managing Director, National Cybersecurity FFRDC

NCF performs applied research and engineering for our sponsors and partners. These strong relationships drive the trust that's needed to build greater impact across industry. We give businesses and organizations practical tools to implement cost-effective, repeatable, and scalable approaches for securing their critical systems.

Our success requires the contributions of select multidisciplinary teams who bring expertise not just in cybersecurity, but also communications, industrial psychology, social sciences, project management, and more. Here are just a few examples of NCF's work addressing existing and emerging cybersecurity challenges.

Artificial Intelligence
NCF worked with industry and academia to develop a taxonomy of concepts and terminology on adversarial machine language that may cause malfunctions in machine learning models. This project enables NIST to develop technical standards and tools that will support reliable and trustworthy systems using AI technologies.

Internet of Things
Billions of devices—from smart phones and wearables to home appliances—populate the Internet of Things (IoT) in personal, military, healthcare, and industrial domains. As those numbers grow, so do security concerns. NCF focused on Consumer Home Internet of Things Product Security to create a repeatable way to assess home IoT devices and their ecosystems. NIST included this in a resource that inspired device manufacturers to implement security capabilities for mitigating cybersecurity issues. Another report provides guidance to help mitigate denial of service attacks that exploit IoT devices in the home.

Election Integrity
Leaders at all levels of government are increasingly concerned about cyber attacks threatening the integrity of our elections, damaging our national security and standing as a global leader. NCF is working with states to analyze impediments to making voting systems more secure. In addition, MITRE is conducting continuing research on securing complex voter registration database systems against adversaries intent on disrupting elections. This research and engineering provides actionable guidance for officials preparing for both near term and future elections.

Securing Space
The launch of massive new commercial satellite constellations in low Earth orbit is driving a need for knowledge about their cyber vulnerabilities. Led by NCF, MITRE is a founding member of the Space Information Sharing and Analysis Center (Space ISAC). Space ISAC is establishing a space systems vulnerability laboratory for its members and analysts from the National Cybersecurity Center in Colorado Springs, Colorado. It will host an unclassified portal where companies can share and analyze adversary tactics and successful defenses. NCF is also working to protect space assets and support government and commercial space initiatives.

ENABLING CAPABILITIES ACROSS THE DIGITAL LANDSCAPE

NCF supports NIST by advancing and promoting standards-based adoption of innovative cybersecurity technologies.

		Health	Energy	Transportation	Election Security	DoD
WHERE WE WORK						
CAPABILITIES WE PROVIDE	Cyber Resiliency	●		●		●
	Privacy	●		●	●	
	AI					●
	IoT/MUD	●				
	Zero Trust					
	5G Cybersecurity			●		
	Transport Labor Security	●		●	●	
	Data Security	●			●	●
WHAT WE DELIVER	Practice Guides	●	●			
	Cybersecurity Framework	●	●	●	●	
	Privacy Framework	●		●	●	
	MITRE ATT&CK™					●

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®