

National Cybersecurity Federally Funded Research and Development Center Strengthening Public Sector Cybersecurity

The National Cybersecurity Federally Funded Research and Development Center (NCF) supports the mission of the NCCoE at NIST—to collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs.

NIST sponsors the NCF to meet cybersecurity research and development needs—and to help demonstrate integrated cybersecurity that is cost-effective, repeatable, and scalable. As an FFRDC, NCF operates in the public interest with objectivity and no organizational conflicts of interest.

Independent | Conflict-Free
Cybersecurity Expertise

MITRE
www.mitre.org

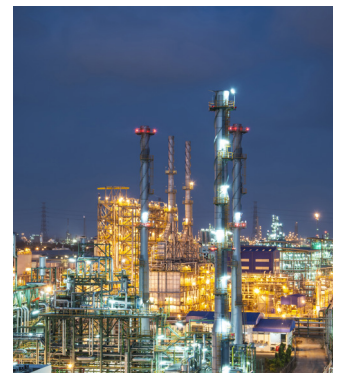
To address today’s most pressing cybersecurity challenges, government agencies can now access the unique facilities, cybersecurity technologies and expertise of the National Cybersecurity Federally Funded Research and Development Center (NCF). The NCF is dedicated to accelerating the adoption of cybersecurity technologies.

The **Work for Others** program, governed by the Program Management Office (PMO) at the National Cybersecurity Center of Excellence (NCCoE), facilitates engagement with the NCF for contributions to complex and critical cybersecurity programs and initiatives.



Who May Use the NCF?

- Federal Agencies
- State Governments
- Municipal Governments
- Not-for-Profit Organizations



Task Areas

NCF provides research, development, engineering, and technical support, such as:

- **Frameworks and implementation strategies** to encourage and expedite adoption of effective cybersecurity controls and mechanisms
- **Collaboration across government, industry, and academia** to accelerate effective innovation
- **Systems engineering and technology testing** to accelerate adoption of cybersecurity technologies by government and private sectors
- **Support for technology transfer** of cybersecurity solutions



How to Get Started

1. Submit an Inquiry

If you are interested in utilizing the FFRDC and its cyber-security capabilities, please email the NCCoE PMO at FFRDCRequests@NIST.gov.

2. Submit A Request

Request a needs assessment form by emailing the NCCoE PMO at FFRDCRequests@NIST.gov.

3. Requests Reviewed

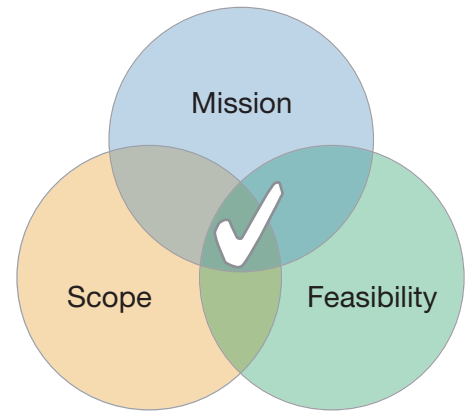
Needs assessment is reviewed to ensure it is within scope of the NCF IDIQ contract* and meets the additional criteria shown below.

4. Inter-Agency Agreement (IAA) Prepared

This is an assisted acquisition. The NCCoE PMO will collaborate with your agency to prepare any necessary documentation for an IAA (e.g., SOW; IGCE; Market Research Report; FMS Forms 7600A and B.)

5. Proposal Submission and Task Order Award

The NIST Acquisition Management Division will issue an RFP to The MITRE Corporation. We will work with your agency to negotiate for the best value in terms of cost and technical approaches. A Task Order will be awarded to MITRE for the approved work proposal.

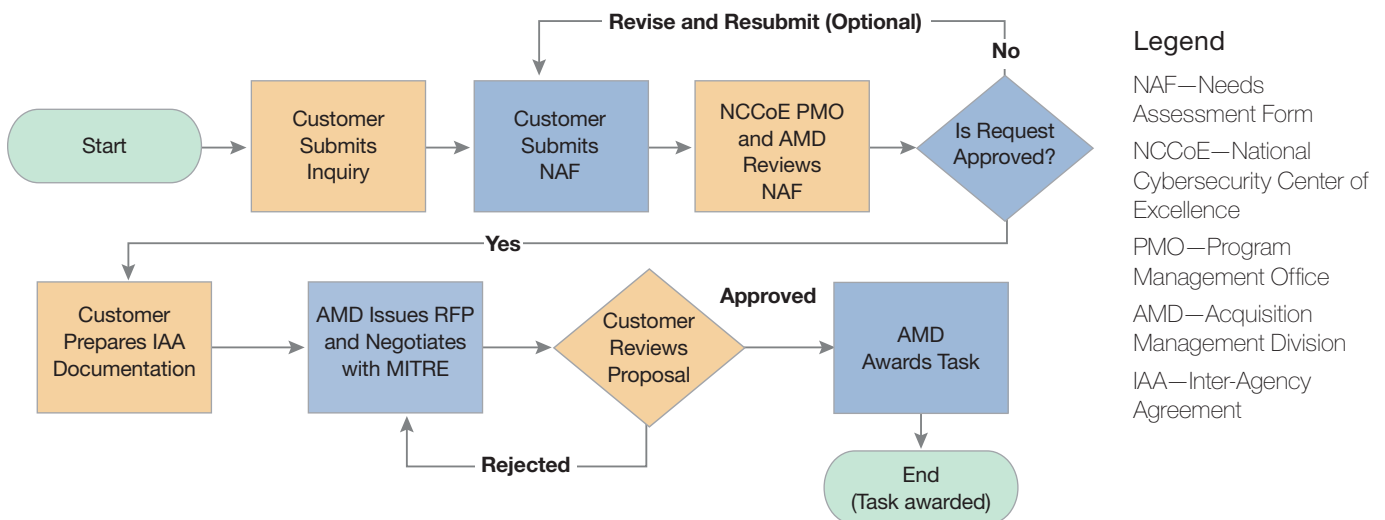


Requests for support are reviewed for scope, consistency with NCF/NCCoE mission, and feasibility.

For more information, please visit <https://www.nccoe.nist.gov/wfo> or email FFRDCRequests@nist.gov.

*NIST Indefinite Delivery, Indefinite Quantity contract no. SB1341-14-CQ-0010.

Ordering Process



Legend

NAF—Needs Assessment Form
 NCCoE—National Cybersecurity Center of Excellence
 PMO—Program Management Office
 AMD—Acquisition Management Division
 IAA—Inter-Agency Agreement