GERALD E. CONNOLLY
11TH DISTRICT, VIRGINIA
2265 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-1492

FAIRFAX OFFICE:
10680 MAIN ST
SUITE 140
FAIRFAX, VA 22030

Congress of the United States
House of Representatives
Washington, DC 20515–4611

HOUSE COMMITTEE ON OVERSIGHT
AND ACCOUNTABILITY
SUBCOMMITTEES:
RANKING MEMBER, CYBERSECURITY,
INFORMATION TECHNOLOGY, AND
GOVERNMENT INNOVATION
GOVERNMENT OPERATIONS
AND THE FEDERAL WORKFORCE

HOUSE COMMITTEE ON FOREIGN AFFAIRS
SUBCOMMITTEES:
INDO-PACIFIC
MIDDLE EAST, NORTH AFRICA, AND CENTRAL ASIA

May 10, 2024

The Honorable Tom Cole
Chairman
Committee on Appropriations
Washington, D.C. 20515

The Honorable Rosa DeLauro
Ranking Member
Committee on Appropriations
Washington, D.C. 20515

Dear Chairman Cole and Ranking Member DeLauro,

I am requesting funding for Internet Name Space Observatory (INSO) in fiscal year 2025. The entity to receive funding for this project is George Mason University, located at 4400 University Drive, Fairfax, VA 2230.

Project: Internet Name Space Observatory (INSO)
Recipient: George Mason University, 4400 University Drive, Fairfax, VA, 22030
Amount: $1,000,000
Background: The Internet Namespace Security Observatory (INSO) will be a first-in-the-nation center to focus research on DNS Security Extensions (DNSSEC) adoption and Domain Name System security and resiliency with the objectives of strengthening the Domain Name System and Internet against cyber-attacks. The INSO will produce foundational research on the alternative strategies for Domain Name System resilience that will provide a quantitative basis for DNS operators to decide on increased investment and technology evolution paths including for DNSSEC adoption. NIST developed the “Security and Privacy Controls for Information Systems and Organizations” (SP 800-53), mandating DNS Security Extensions (DNSSEC), the “Secure Domain Name System (DNS) Deployment Guide” (SP 800-81-2), Zero Trust Architecture guidance (SP 800-207), and the NIST Cybersecurity Framework. These NIST initiatives include two DNSSEC related security controls (SC-20 and SC-21, in SP 800-53) and the development of the Framework for Improving Critical Infrastructure Cybersecurity and the Secure Software Development Framework, new standards for personal data security regulation and digital identity research. In addition, NIST’s High Assurance Domains (HAD) project illustrated the innovation potential that vibrant DNSSEC deployment enables. Research results from the INSO including near real time monitoring of Domain Name System operations with the INSO Cybersecurity Operations Center will help to formally quantify cybersecurity and resilience benefits that are being derived from DNS investment, DNSSEC adoption, and cybersecurity policies and mandates. In this way, the INSO will contribute to protecting and enabling technology innovations by safeguarding the security of critical Internet Domain Name Infrastructure. This project is a good use of taxpayer dollars because it is consistent with both recent and longstanding federal cybersecurity priorities. NIST SP 800-53 mandates DNSSEC deployment throughout .gov domains, and the INSO will produce research results that will illustrate the benefits of, and lead to new innovations in, these deployments. In addition, Executive Order 14028 outlines several priorities addressed by the INSO and its DNS focus: removing barriers to Cybersecurity Threat Intelligence (CTI) sharing, modernizing cybersecurity with Zero Trust Architectures (ZTA),

enhancing supply chain security, and establishing a Cyber Safety Review Boards. Further, the Executive Office of the President previously issued OMB Memorandum M-08-23, mandating the Domain Name System's (DNS') Security Extensions (DNSSEC) for all .gov domains. The INSO's focus on safeguarding the DNS is critical in enabling these priorities, and also as a foundation for other enhanced protections. As the DNS is foundational in Internet operations, the INSO will directly lead to and stimulate, novel research results that will include novel Zero-Trust CTI, secure vehicle-to-everything (V2X) communications for aerial and automotive sectors, security for enhanced Mobile Broadband over 5G, and secure healthcare platforms.

The project has a Federal nexus because the funding provided is for the purposes authorized by 272 of title 15, United States Code.

I certify that I have no financial interest in this project, and neither does anyone in my immediate family.

Best Regards,

Gerald E. Connolly

Gerald E. Connolly
Member of Congress
11th District, Virginia