Committee on Energy and Commerce
U.S. House of Representatives

Witness Disclosure Requirement - "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

1. **Your Name:** Zachary D. Tudor

2. **Your Title:** Associate Laboratory Director, National and Homeland Security, Idaho National Laboratory

3. **The Entity(ies) You are Representing:** The Idaho National Laboratory which is a federally funded research and development center owned by the U.S. Department of Energy. The INL is managed and operated by Battelle Energy Alliance, LLC, under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy.

4. **Are you testifying on behalf of the Federal, or a State or local government entity?**	**Yes**	**No** X

5. **Please list any Federal grants or contracts, or contracts or payments originating with a foreign government, that you or the entity(ies) you represent have received on or after January 1, 2015. Only grants, contracts, or payments related to the subject matter of the hearing must be listed.**

a) Korea Atomic Energy Research Institute (KAERI): Assess and develop concepts for potentially reducing Nuclear Facility I&C (Instrument and Control) systems vulnerabilities.
b) Emirates Nuclear Energy Corporation: Evaluate each Advanced Pressurized Water Reactor installation for resilient and secured systems to protect the Barakah NPP national assets for ENEC.
c) Department of Energy and Climate Change, United Kingdom: Industrial control systems cyber security training.

6. **Please attach your curriculum vitae to your completed disclosure form.**

Signature:[redacted] **Date:** 3/9/18

ZACHARY D. TUDOR, CISSP, CCP, CISM, IAM/IEM

[redacted]

Executive Summary

Operational Technology Executive with more than 20 years of experience working in the federal and commercial sectors in information security, network security, technical program management, research and development, technical training, and computer system operation and maintenance. Deep understanding of Computer Network Defense operations, Security Architecture Development, Certification and Accreditation, Disaster Recovery and Business Continuity, and IT systems auditing. Proven success working with federal clients in the Intelligence Community, the Departments of Defense, Treasury, Justice, Health and Human Services, Transportation, and Homeland Security, and has commercial clients in the technology infrastructure and financial services industries.

Experience

Idaho National Laboratory, Idaho Falls, ID **2016 – Present**

Associate Laboratory Director, National and Homeland Security

Responsible for leadership, management, and operations of INL's major center for national security technology development and demonstration, employing 500 scientists and engineers across $300M in programs. N&HS is responsible for INL's Nuclear Nonproliferation, Critical Infrastructure Protection, Defense Systems, and Homeland Security missions. These missions include safeguarding and securing vulnerable nuclear material, enhancing the overall security and resilience of the nation's infrastructure, and providing protective system solutions and heavy manufacturing of armor for national defense. N&HS supports major programs for the Department of Defense (DOD), Department of Homeland Security (DHS), and the Intelligence Community.

SRI International, Arlington, VA **2008 – 2016**

Program Director, Computer Science Laboratory

Reporting to the Lab Director, management and technical resource for operational and research and development cyber security programs for government and commercial customers including the Department of Homeland Security Cyber Security Research and Development Center (CSRDC), DARPA, and the National Cyber Range. Projects and accomplishments include:

- Coordination and subject matter expertise for the LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) consortium. Project manager for the LOGIIC Safety Instrumented System (SIS) project. On-site technical manager for Third Party Access project assessments. Selected Accomplishments:
- Represents SRI at the International Information Integrity Institute (I-4), a world forum for senior information security professionals to share cyber information.
- Member of the Nuclear Cyber Security Working Group, and contributing author of the 2011 Nuclear Cybersecurity Roadmap
- Co-leader of SRI's team on the National Electric Sector Cybersecurity Organization Resource (NESCOR), a broad-based public-private partnership with the Department of Energy (DOE) to strengthen the cyber security posture of the electric sector.
- Former co-chair of the Industrial Control System Joint Working Group (ICSJWG) R&D working group

- Project manager for the DHS and White House sponsored Financial Industry Validation of Identity Credential Services (FI-VICS) project
- Member of the Department of Defense Research and Engineering (DDR&E) special study group on cybersecurity metrics (2010)
- Conduct innovation workshops based on SRI's Five Disciplines of Innovation for DHS and National Lab cybersecurity researchers
- Coordination and chapter author for the 2009, DHS S&T document *A Roadmap for Cybersecurity Research*

Securicon, LLC 2006 – 2008

Director, Homeland Security Services

Managed team of five senior security engineers at the Department of Homeland Security National Cyber Security Division and serve as cyber security expert. The team provided program management and control systems cyber security expertise and support for the Control Systems Security Program, and operational support to the US-CERT in managing cyber threats, incidents and vulnerabilities. Supported Securicon clients conducting engagements in security architecture development, system certification and accreditation, security audits and assessments. Oversaw the development of security solutions to address each client's unique network and security architecture to satisfy clients' security requirements while also supporting their functional business requirements.

Global Professional Solutions, Inc. 2005 – 2006

Provided management oversight, personnel management, and quality assurance for deliverables for customers in the Federal Government, primarily the Department of State and Drug Enforcement Agency. Assisted with business development efforts for all customer sectors, including Intelligence and Defense. Developed business relationships and company partnerships to create new service offerings.

Bearing Point 2004 – 2005

Senior Manager, Information Assurance Practice

Senior managing consultant for the BearingPoint Information Assurance Practice, responsible for Department of Defense, Intel, and Homeland Security information security projects such as security program development and implementation, coordination and development of IA documentation for Systems Security Authorization Agreements (SSAAs), risk assessment and mitigation reports, Security Test and Evaluation (ST&E) plans, contingency, business continuity, and disaster recovery plans, and IA policies and procedures. Responsible for and participated in a wide range of Information Assurance consulting assignments covering operational security, certification and accreditation, and security management. Senior InfoSec consultant for the Defense Finance and Accounting Service (DFAS) Forward Compatible Payroll (FCP) project, the Department of Justice Audit Support project, and OSD CIO Information Architecture security review. Technical lead for the US Army European Command (EUCOM) requirements development and implementation of a multi-level secure (MLS) exercise environment using Sun's Trusted Solaris operating system and Secure Network Access Platform (SNAP) architecture.

Computer Associates 2004

Senior Project Manager

Provided Information Security program management for federal government software integration and staff augmentation projects. Develop proposals and statements of work for project work. Coordinates activities of product experts (consultants) for customer trial and demonstration engagements. Project manager for Computer Associates on-going software integration support to the Federal Aviation Administration's Computer Security Incident Response Center (CSIRC), and to Internal Revenue Service and Social Security Administration projects.

George Mason University 2003 – 2007

Adjunct Professor, School of Information Technology and Engineering

Taught courses for the Information Security M.S. program including "Intrusion Detection Systems", "Special Topics in Denial of Service" and "Information Security Principles".

CACI 2003 – 2004

Senior Information Security Engineer

Provided Information Security management and consulting for corporate and government projects. Information Systems Security Officer (ISSO) for the Office of the Secretary of Defense Chief Information Officer (OSD/CIO) Enterprise Operations Support Team (EOST). Responsible for operational information security for OSD/CIO classified and unclassified network, compliance with Department of Defense information security regulations, and first level incident response. Developed plans (DITSCAP SSAA), policies and architectures for OSD/CIO network systems. Conducted security briefings and training for IA and EOST staff. Responsible for maintaining Vulnerability Management System (VMS) compliance, identifying and resolving system vulnerabilities using automated tools including ISS Scanner, Microsoft Baseline Security Analyzer (MBSA), and Nessus vulnerability scanner. Performed operating system hardening processes according to established Security Technical Implementation Guidelines (STIGs), deployed security patches, and coordinated anti virus support for desktops and servers. Performed Certification and Accreditation activities, security policy development, and incident response for the Bureau of Indian Affairs.

Lockheed Martin 2002 – 2003; 1996 - 1998

Manager, Data Security 2002 - 2003

Manager for security operations for the Centers for Medicare and Medicaid Services (CMS) through the CITIC contract. Through CITIC, CMS outsourced the management and operations of its network and data center environment consisting of IBM mainframes (OS/390 and Z/OS), Windows 2000, Solaris and AIX network servers, over 5,400 user PCs, and 11 regional office LANs. The ten-person security team provides administration and operation for security devices including: firewalls (Nokia Checkpoint and AIX Checkpoint), proxy servers, network virus scanning systems, switch and router ACLs; monitoring and alert response for Intrusion Detection Systems (IDS); oversight of desktop, server, network, regional, and mainframe security; and engineering studies and recommendations for security infrastructure improvement.

Deputy Program Manager, Computer Systems Branch, Program 431 1996 - 1998

Deputy Director of a 230-person information technology (IT) organization. This $40M per year organization provided continuous, 24-hour computing services and network monitoring and operations to customers in support of National Reconnaissance Office (NRO) operations. Personally responsible for daily operations and management of all internal aspects of the program.

Predictive Systems 2002

Principle Consultant

Provided Information Security consulting and program management for corporate and government projects. Project manager for the Department of Justice Information Sharing and Analysis Center (ISAC), which provided the DOJ early warning and information on information security threats and vulnerabilities. Project manager for the MSC-ISAC, a similar service aimed at serving all government agencies. Managed the installation, activation and monitoring of new perimeter network security for the Bureau of Indian Affairs following the court ordered shutdown of agency internet access due to poor security infrastructure. Lead consultant for an assessment of perimeter network (DMZ) security for the World Bank.

U.S. Alliance Group 2000 – 2001

Vice President, Operations

Responsible for management of all operational aspects of this start-up technical recruiting firm. Oversaw company infrastructure including telephone, network and office support equipment installation and maintenance agreements. Primarily responsible for customer satisfaction, including position requirement determination and candidate placement.

- Personally directed 8 technical recruiters and provided overall management for company personnel.
- Led training and orientation sessions on network operations, LAN/WAN configurations, and applicable standards (BCSI, TIA, EIA) for recruiting staff.
- Personally screened candidates for hard fill and high value technical assignments.

SAIC 1998 – 2000 and again in 2001

Vice President, Program Management, Division Manager

Program manager for the Department of Transportation (DOT) Year 2000 Service Bureau (Y2KSB), a $24M task order contract under the ITOP contract, and its follow-on, the Millennium Solutions Center (MSC). Responsible for division profit and loss and the management of over 125 SAIC and contractor personnel, performing on 21 tasks for clients including the Executive Office of the President, the Securities and Exchange Commission, the National Archives, the Federal Aviation Administration, the Environmental Protection Agency, and the U.S. Coast Guard. The Service Bureau supports government customers in performing Y2K related services, including program management, business continuity and contingency planning, legacy code assessment, remediation and renovation, hardware and software inventories, on-site system remediation assistance, and independent verification and validation of Y2K remediation programs. Selected Accomplishments:

- Directed the development of Business Continuity and Contingency Plans (BCCPs) and Continuity of Operations Plans (COOP) for the Executive Office of the President and the President's Council on Y2K Conversion.
- Managed the development of a new Enterprise Architecture for the National Archives and Records Administration.
- Managed Independent Validation and Verification (IV&V) of software and system compliance of all critical systems for the FAA, EPA, SEC, and USCG.
- Delivery manager and workgroup member for the Department of Treasury's input to the National Infrastructure Protection Plan under PDD-63.

Senior Technical Manager

Senior Information Security Manager supporting the Department of Transportation's Millennium Solution Center. Provide project management for the Information Assurance program support to the Environmental Protection Agency Office of Environmental Information (OEI) and Office of the Chief

Financial Officer (OCFO) and senior information assurance expertise for other project assignments. Selected Accomplishments:

- Served as senior information security advisor for development and ongoing operations of the Department of Justice Computer Incident Response Center, for information security support to the Securities and Exchange Commission.

U.S. Navy 1976 – 1997

Submarine Electronics Officer (LDO/628X), Chief Data Systems Technician

- **Flag Lieutenant/Aide, Commander, Navy Recruiting Command,** (07/96- 12/96). Personal assistant to a Rear Admiral, director of a 5,000-person search and recruit organization in 50 states and 5 overseas locations. Organize and attend senior ranking military and civilian (Fortune 500) meetings, conferences and forums involving Navy recruiting and personnel management. Represent the Executive Staff on the Internet Task Force, coordinating headquarters and field activities' strategic use of emerging technology.
- **Head, Submarine Electronic and Diver Training Programs, Chief of Naval Operations (N879),** (08/94-06/96). Director of training programs for submarine electronic, navigation, exterior and interior communication, hull and mechanical systems and cryptologic systems. Responsible for requirements determination, planning, programming and budgeting for 175 courses at seven submarine training sites with a $16M annual budget. Directed the manpower and training consolidation of submarine electronic technicians into a single training track, effecting over 50 courses of instruction at six submarine training sites, with projected savings of over $5M over 3 years. Project Officer for the Virtual Environment for Submarine Training, a $4M Research and Development effort using virtual reality to simulate submarine navigation.
- **Training Acquisition Manager, Submarine Electronic Support Measures (ESM) Training, Naval Sea Systems Command (PMS 425)** (11/92-07/94). Training acquisition manager for 16 submarine force and Naval Security Group electronic warfare systems. Contracting Officers Technical Representative (COTR) for submarine ESM systems. Developed and contracted curriculum materials. Developed Interactive Courseware, Computer Based Training, and Integrated Electronic Technical Manuals for submarine ESM and cryptologic systems.
- **Information Systems Manager/Information Security Officer (ISO), Naval Submarine Training Center Pacific** (07/90-10/92). Managed operations, programming and support staff providing personal computers, LANs and WANs. LAN administrator for Digital Equipment PCSA and Novell systems. Prepared Abbreviated System Decision Papers (ASDPs) for hardware acquisition. Student control officer for 30,000 students annually. Developed and implemented Information System security plans. Created and tested disaster and contingency plans to ensure system availability. Prepared and conducted training for Information System security officers.

Education

- M.S., Information Systems, George Mason University
- Ph.D. Studies (ABD) Information Security, George Mason University
- Graduate Certificate in Information System Security, George Mason University
- B.S., Computer Software, Regents College

Professional Certifications

- Certified Information Systems Security Professional (CISSP), 2000
- Project Management Professional (PMP), 2004 - 2010
- Certified Information Security Manager (CISM), 2004

- Certified in the National Security Agency's InfoSec Evaluation Methodology (IEM), and InfoSec Assessment Methodology (IAM), 2004
- Certified Computer Professional (CCP), 1997
- Master Training Specialist (Department of the Navy), 1984

Security Clearance

- Top Secret/SCI with Full Scope Polygraph

Other Activities

- National Academies of Science and Engineering; Air Force Studies Board (AFSB), January 2018 – Present
- International Information Systems Security Certification Consortium [(ISC^2)]; Board of Directors, January 2017 - Present
- Hawaii Intergovernmental Information Processing Council (A FGIPC member) – Vice President (1992)
- National Naval Officers Association – National Board of Directors (1992-1993)

Idaho National Laboratory INL

Zachary (Zach) Tudor

Associate Laboratory Director
National & Homeland Security
Idaho National Laboratory

Tudor is responsible for Idaho National Laboratory's (INL) National and Homeland Security (N&HS) mission. N&HS is a major center for national security technology development and demonstration, employing 500 scientists and engineers across $300M in programs at the lab. He is responsible for INL's Nuclear Nonproliferation, Critical Infrastructure Protection and Defense Systems missions. These missions include heavy manufacturing of armor, application of INL's full-scale and unique infrastructure (grid, wireless testbed, explosives range, and a number of research facilities). In addition to the Department of Energy, these missions also support major programs for Department of Defense, Department of Homeland Security, and the Intelligence Community.

Previously, Tudor served as Program Director in the Computer Science Laboratory at SRI International, where he acted as a management and technical resource for operational and research and development cybersecurity programs for government, intelligence and commercial projects. He supported DHS's Cyber Security Division on projects including the Linking the Oil and Gas Industry to Improve Cybersecurity consortium, and the Industrial Control System Joint Working Group R&D working group. He has served as a member of (ISC)2's Application Security Advisory Board and the NRC's Nuclear Cyber Security Working Group, as well as the Vice Chair of the Institute for Information Infrastructure Protection at George Washington University.

Prior to SRI, Tudor led a team of cybersecurity engineers and analysts directly supporting the Control Systems Security Program at DHS, whose mission is to reduce the cybersecurity risk to critical infrastructure systems. Past assignments include on-site deputy program manager for the National Reconnaissance Office's world-wide operational network, information security manager for the Secretary of Defense's Chief Information Officer's Enterprise Operations Support Team; security management support for the Centers for Medicare and Medicaid Services; and several senior-level consulting positions including Vice President of SAIC's Enabling Technology Division, and Senior Manager for DOD programs at Bearing Point's Security Practice.

A retired U.S. Navy Submarine Electronics Limited Duty Officer and Chief Data Systems Technician, Tudor holds an M.S. in Information Systems from George Mason University concentrating in cybersecurity, where he was also an adjunct professor teaching graduate courses in information security.

His professional credentials include the Certified Information Systems Security Professional, Certified Information Security Manager and Certified Computer Professional. Tudor can be reached at:

Idaho National Laboratory
P. O. Box 1625-MS 3750
Idaho Falls, ID 83415
(208) 526-5051
Zachary.Tudor@inl.gov