Controlled Unclassified Information (CUI) Security Requirements Workshop Program

Thursday, October 18, 2018
8:30 AM – 5:00 PM Eastern

NIST Red Auditorium
100 Bureau Drive, Gaithersburg, MD 20899

Workshop Purpose: The National Institute of Standards and Technology (NIST), in coordination with the Department of Defense (DoD) and the National Archives and Records Administration (NARA), is hosting an informational workshop providing an overview of Controlled Unclassified Information (CUI), the Defense Acquisition Regulations System (DFARS) Safeguarding Covered Defense Information and Cyber Incident Reporting Clause, and NIST Special Publications 800-171 and 800-171A. This workshop will also feature panels of Federal Government representatives discussing expectations for evaluating evidence and implementing the CUI Security Requirements, and industry representatives sharing best practices and lessons learned.

CUI Security Requirements Workshop Program

Workshop Agenda with Presentation Abstracts **2**

Speaker Profiles **5**

Additional Workshop Information and Resources **10**

Workshop Agenda with Presentation Abstracts

7:30 AM **Registration Opens** - *Red Auditorium Lobby*

8:30 AM – 8:45 AM **Welcome to NIST,** *Dr. Charles Romine, Director, Information Technology Laboratory (ITL), NIST*

Dr. Romine will provide a welcome and overview of the NIST mission and organization, overview of the ITL, and highlight the portfolio cybersecurity research programs within the ITL.

8:45 AM – 9:30 AM **Opening Keynote – Protecting the Nation's Critical Information: One Team, One Mission,** *Dr. Ron Ross, NIST Fellow, Information Technology Laboratory, NIST*

As we push computers to "the edge" building an increasingly complex world of interconnected information systems and devices, security and privacy continue to dominate the national dialogue. The Defense Science Board in its 2017 report, *Task Force on Cyber Defense*, provides a sobering assessment of the current vulnerabilities in the U.S. critical infrastructure and the information systems that support the mission essential operations and assets in the public and private sectors. There is an urgent need to further strengthen the underlying information systems, component products, and services that the nation depends on in every sector of the critical infrastructure—ensuring those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. Today, the cybersecurity threat from determined adversaries looms large in all sectors of the United States critical infrastructure. As with all existential threats faced by this nation throughout history, we must mobilize the essential partnership—government, industry, and the academic community to provide the people, processes, and technologies necessary to protect our critical national assets. One team, one mission.

9:30 AM – 10:30 AM **Overview of Controlled Unclassified Information (CUI), the CUI Registry, and the CUI Rule,** *Devin Casey, Program Analyst, Controlled Unclassified Information, Information Security Oversight Office, National Archives and Records Administration (NARA)*

This presentation will cover the CUI program and plans for oversight for both the executive branch as well as in industry. Topics range from the distinctions between CUI and Proprietary information to agencies implementation efforts and general timelines for phased implementation of CUI in the federal environment as well as in industry through contracts.

10:30 AM – 10:45 AM **Break –** *Coffee and snacks available for purchase in the NIST Cafeteria*

10:45 AM – 11:45 AM **Overview of the Defense Acquisition Regulations System (DFARS) Safeguarding Covered Defense Information and Cyber Incident Reporting Clause,** *Vicki Michetti, Director, Cybersecurity Policy, Strategy and Defense Industrial Base Cybersecurity Program, Department of Defense (DoD) and Mary Thomas, Program Analyst, Director of Defense Procurement and Acquisition Policy, Office of the Under Secretary of Defense, DoD*

This presentation will address DoD's implementation of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." DoD Contractors are required to provide "adequate security" for covered defense information associated with contracts that contain DFARS Clause 252.204-7012. These security requirements are found in NIST Special Publication 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations." The clause also requires DoD contractors to report to the Department when the

contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.
In addition, this session will address:

- Covered defense information
- Implementing NIST SP 800-171 security requirements, specifically the requirement for a system security plan
- Contractor compliance with DFARS Clause 252.204-7012 and the requirement to implement NIST SP 800-171 not later than December 31, 2017
- DoD's Defense Industrial Base Cybersecurity Program
- Resources to assist in the implementation of DFARS Clause 252.204-7012

11:45 AM – 12:45 PM Overview of NIST Special Publication (SP) 800-171, Protecting CUI in Nonfederal Systems and Organizations, *Devin Casey, Program Analyst, Controlled Unclassified Information, Information Security Oversight Office, NARA; Kelley Dempsey, Senior Information Security Specialist, NIST; and Gary Guissanie, Adjunct Research Staff Member, Institute for Defense Analysis*

This presentation will provide an overview of the set of recommended security requirements for protecting the confidentiality of CUI, highlight recent errata updates to include a new appendix that contains an expanded discussion about each CUI requirement, and additional supplemental materials (CUI System Security Plan template, Plan of Action template, and mapping between the Cybersecurity Framework and SP 800-171 security requirements) available on the NIST Computer Security Resource Center (https://csrc.nist.gov).

12:45 PM – 1:45 PM Lunch – *Available for purchase in the NIST Cafeteria*

1:45 PM – 2:30 PM Overview of NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, *Kelley Dempsey, Senior Information Security Specialist, NIST and Victoria Yan Pillitteri, Computer Scientist, NIST*

This presentation will provide an overview of NIST SP 800-171A, which provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST SP 800-171.

2:30 PM – 2:45 PM Break – *Coffee and snacks available for purchase in the NIST Cafeteria*

2:45 PM – 3:45 PM Government Panel: Expectations for Evaluating the Implementation of CUI Security Requirements in NIST SP 800-171, *Devin Casey, Program Analyst, Controlled Unclassified Information, Information Security Oversight Office, NARA; Kelley Dempsey, Senior Information Security Specialist, NIST; Vicki Michetti, Director, Cybersecurity Policy, Strategy and Defense Industrial Base Cybersecurity Program, DoD; Mary Thomas, Program Analyst, Director of Defense Procurement and Acquisition Policy, Office of the Under Secretary of Defense, DoD; Moderated by Patricia Toth, Cybersecurity Program Manager, Manufacturing Extension Partnership, NIST*

This panel will discuss how to effectively evaluate the implementation of the CUI Security Requirements in NIST SP 800-171. Panelists will provide insight on expectations and challenges of implementing SP 800-171 in a variety of environments.

3:45 PM – 5:00 PM Industry Implementation of CUI Security Requirements: Best Practices and Lessons Learned, *Kristin Grimes, Corporate Counsel, Leidos; Gaurav Pal, CEO and Founder, Stackarmor; Vijay Takanti, Senior Vice President, Product Development, Exostar; Moderated by Robert Metzger, Attorney, Rogers Joseph O'Donnell, P.C.*

NIST created SP 800-171 for commercial organizations to protect federal Controlled Unclassified Information (CUI). Defense contractors already are required to protect CUI. Civilian agencies are moving to impose similar obligations on hundreds of thousands of non-federal entities who have CUI. This panel will present the perspective, predictions and recommendations of industry experts. Focusing first on critical challenges, and successful compliance strategies, the panel then will advise on how companies can demonstrate and sustain security and discuss ways to leverage SP 800-171 safeguards and use the SP 800-171A assessment guide to elevate and expand security over time, respond to the always changing threat environment and satisfy rising government expectations.

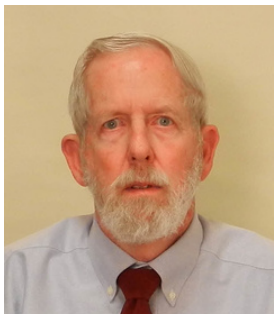
Speaker Profiles

Devin Casey is a Program Analyst for the Information Security Oversight Office (ISOO) at the National Archives and Records Administration. He serves as a lead for implementation and oversight activities for the Controlled Unclassified Information (CUI) Program. He came to the National Archives from the US Department of Agriculture where he worked in their Classified National Security Programs Branch. He also serves in the Army reserves as an intelligence analyst and security manager with tactical and strategic experience. In his current role at ISOO, he consults with Executive branch departments, agencies, and industry as well as other non-federal organizations on the structure and implementation of the CUI program.

Kelley Dempsey began her career in IT in 1986 as an electronics technician repairing computer hardware before moving on to system administration, network management, and information security. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program, and then joined the NIST Computer Security Division FISMA team in October 2008. Kelley has co-authored NIST SP 800-128 (Security-Focused Configuration Management), NIST SP 800-137 (Information Security Continuous Monitoring), NISTIR 8011 (Automating Ongoing Assessments), and NISTIR 8023 (Risk Management for Replication Devices), and is a major contributor to NIST SPs 800-30 Rev 1, 800-37 Rev 1, 800-53 Rev 3/Rev 4, 800-53A Rev 1/Rev 4, 800-39, 800-160, and 800-171. Kelley earned a B.S. in Management of Technical Operations, graduating cum laude in December 2003, and an M.S. in Information Security and Assurance in December 2014. Kelley also earned a CISSP certification in June 2004, a CAP certification in January 2013, and a Certified Ethical Hacker certification in November 2013.

Kristin Grimes is corporate counsel at Leidos, specializing in cyber issues from the program to enterprise level and throughout the Leidos supply chain. She advises stakeholders on best practices, incident response, and all aspects of cyber regulatory compliance. Ms. Grimes is also responsible for litigation, e-Discovery, insider threat mitigation, and domestic and international investigations, including privacy implications. Prior to joining the Legal department in 2013, Ms. Grimes spent ten years with SAIC/Leidos working operational and strategic counterintelligence, counterterrorism, and cyber issues for the U.S. Intelligence Community.

Ms. Grimes is an advocate for pro bono service and founder of the Leidos Pro Bono Program. She is also a member of the Intelligence and National Security Alliance (INSA) Legal Working Group and Insider Threat Subcommittee, as well as a Vice Chair for the American Bar Association Public Contract Law Cybersecurity, Privacy, and Data Protection Committee. Ms. Grimes received her J.D. from The George Washington University Law School and has a B.A. in Political Science/Japanese and an M.A. in International Relations from Seton Hall University.



Gary Guissanie served 20 years as a US Army Signal Officer (Communications-Electronics Systems Engineer) with various tactical communications, communications systems engineering and project management assignments in the Army, NATO, the National Security Agency and White House; 20 years as a DoD civilian engaged in emergency operations planning, critical infrastructure protection and information assurance / cybersecurity at the White House and Office of the Secretary of Defense, culminating in responsibility for oversight of all cybersecurity / information assurance for the DoD as Acting Deputy Assistant Secretary of Defense for Identity and Information Assurance. He is currently a "Special Government Employee – Consultant" to the DoD CIO on cybersecurity matters and an Adjunct Research Staff Member at the Institute for Defense Analyses (IDA), a Federally Funded Research and Development Center, focused on the cybersecurity aspects of information technology and systems development. Co-Author, with NIST and NARA, of NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Mr. Guissanie has a Bachelor of Science in Physics from the Polytechnic Institute of Brooklyn, a Master of Science in Systems Management from the University of Southern California, and a Master of Science in National Resource Strategy from the National Defense University Industrial College of the Armed Forces/School of Information Warfare and Strategy.

Vicki Michetti is the Director of Cybersecurity Policy, Strategy, International Engagement, and the Defense Industrial Base (DIB) Cybersecurity Program, under the DoD Chief Information Officer. She joined the Office of the Secretary of Defense in January 2011. Ms. Michetti has experience working in industry, and over 28 years of federal service, 22 years as a commissioned Air Force officer. Prior to her current position, Ms. Michetti worked in industry as an Information Systems Engineer and as a Program Analyst. Ms. Michetti also had a distinguished military career, having served on the Joint Staff, the Air Staff, and as Commander of the 25th Weather Squadron at Davis-Monthan Air Force Base. Ms. Michetti retired from the United States Air Force in 2007. She is the recipient of numerous military decorations, including the Defense Superior Service Medal. Ms. Michetti earned a Bachelor's degree in Mathematics from California State University, Sacramento, and a Master's degree in Atmospheric Science from Creighton University.

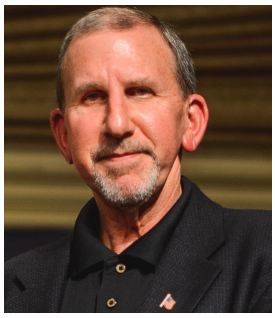
Robert S. Metzger, an attorney in private practice, heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a firm that has specialized in public contract matters for more than 35 years. Bob represents leading U.S. and international technology companies in several industry sectors. Bob attended Georgetown University Law Center, where he was an Editor of the Georgetown Law Journal. Subsequently, he was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School. As a Special Government Employee of the Department of Defense, Bob was a member of the Defense Science Board task force that produced the Cyber Supply Chain Report in April 2017. Bob is recognized for subject area leadership in cyber, supply chain and related security matters and has many publications in these subject areas. Named a 2016 "Federal 100" awardee, Federal Computer Week cited Bob for his "ability to integrate policy, regulation and technology" and said of him: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike." Chambers USA (2018) ranks Bob among top government contracts lawyers and said that "[h]e is particularly noted for his expertise in cyber and supply-chain security with clients regarding him as the 'preeminent expert in cybersecurity regulations and how they affect government

contractors.'" For RSA Conference 2018, Bob served on a panel on "First Recourse or Last Resort? The National Interest in Regulating the IoT" and moderated a second panel on "IOT and Critical Infrastructures: A Collision Of Fundamentals?" For RSAC Conference 2017, Bob moderated a discussion on "Cyber/physical Security and the IoT: National Security Considerations." A member of the International Institute for Strategic Studies (ISS), Bob's articles on national security topics have appeared in International Security and the Journal of Strategic Studies, among other publications. Bob is active in public-private security initiatives including a present assignment under the auspices of The MITRE Corporation, a FFRDC.

Gaurav Pal (G.P.) is a Senior Technology Executive with over 20 years of information systems modernization and implementation experience. He is the principal and co-founder of stackArmor, a security focused cloud solutions firm. G.P. also contributed to Federal cloud initiatives including U.S. Treasury's Public Cloud Webhosting Solutions, Department of the Interior Foundation Cloud Hosting Services, and Recovery.gov 2.0.

Victoria Yan Pillitteri is a computer scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST), where she leads a team of cybersecurity researchers to develop security risk management guidance and publications. She previously worked on the Cybersecurity Framework, led the NIST Smart Grid and Cyber Physical Systems Cybersecurity Research Programs, served on the board of directors of the Smart Grid Interoperability Panel, and served on a detail in the office of the NIST Director as an IT policy advisor. Victoria holds a B.S. in Electrical Engineering from the University of Maryland, a M.S in Computer Science, with a concentration in Information Assurance, from the George Washington University, and is a Certified Information Systems Security Professional (CISSP).

Dr. Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems. ITL develops and disseminates cybersecurity standards and guidelines for Federal agencies and U.S. industry. ITL supports these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics.



Dr. Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). His current focus areas include information security and risk management. Dr. Ross leads the Federal Information Security Management Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical information infrastructure. Dr. Ross is the principal architect of the Risk Management Framework (RMF), a multi-tiered approach that provides a disciplined and structured methodology for integrating the suite of FISMA-related standards and guidelines into a comprehensive enterprise-wide security program. Dr. Ross also leads the Joint Task Force, an interagency partnership with the Department of Defense, the Office of the Director National Intelligence, and the Committee on National Security Systems that developed the Unified Information Security Framework for the federal government and its contractors.

Mary Thomas currently serves as a program analyst for the Director of Defense Pricing and Contracting (DPC), in the Office of the Under Secretary of Defense (Acquisition and Sustainment). In this position, Ms. Thomas is responsible for representing DPAP and the DoD contracting community in matters related to cybersecurity. Prior to her assignment with DPAP, Ms. Thomas served in the Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) and as a Project Engineer at the U.S. Army Belvoir Research, Development and Engineering Center. Ms. Thomas has a Bachelor of Science in Industrial Engineering and Operations Research from Virginia Polytechnic Institute and State University, a Master of Science in Systems Management from the University of Southern California, and a Master of Science in National Resource Strategy from the Industrial College of the Armed Forces at the National Defense University.

Vijay Takanti serves as Senior Vice President of Product Development at Exostar. Vijay is responsible for the strategy and product road map, design, development, and customer delivery of Exostar solutions. Vijay has more than 25 years of experience in electronic data processing, application design and development, and information security solutions. He joined Exostar through the acquisition of Evincible® Software in 2004, where he was the founder and CEO. At Evincible®, Vijay developed solutions that bridge the integration chasm between business applications and security components, such as Public Key Infrastructure (PKI).
Prior to founding Evincible®, Vijay served as Chief Technology Officer (CTO) at the Society of Worldwide Interbank Telecommunication (SWIFT), where he architected the Next Generation of the SWIFT Net architecture. SWIFT is the financial industry-owned cooperative supplying secure messaging services and interface software to more than 7,000 financial institutions in nearly 200 countries worldwide, processing on average an estimated USD 6 trillion of payment messages.
Vijay is recognized as an expert on the evolving technologies related to identity management and cybersecurity. He has engaged with a variety of enterprises on these topics and speaks frequently at industry and technology events. He holds a Bachelor's Degree in Electronics and Communications from JNTU in Hyderabad, India; a Master's Degree in Computer Sciences from the Indian Institute of Technology in Khargpur; and an MBA from George Mason University.

Patricia Toth is the Cybersecurity Program Manager at the NIST Manufacturing Extension Partnership (MEP). She works with MEP Centers nationwide to improve the cybersecurity posture of small manufacturers. Formerly Pat was the lead for the NIST Cybersecurity Small Business Outreach. She served as the Chair of the Federal Information Systems Security Educators' Association (FISSEA) Technical Working Group, and Chair of the Federal Computer Security Program Managers' Forum. Pat has worked on numerous documents and projects during her 28 years at NIST including SP 800-53, SP 800-53A, SP 800-171, SP 800-16 rev 1, NISTIR 7621 and Handbook 162. She is a recipient of the Department of Commerce Gold and Bronze Medal Awards.

Pat holds a Bachelor of Science in Computer Science and Math from the State University of New York Maritime College. She served in the Navy as a Cryptologic Officer. Pat received a Joint Service Achievement Medal for her work on the rainbow series of computer security guidelines while assigned to the National Security Agency.

Additional Workshop Information and Resources

Workshop Website: https://go.usa.gov/xUkXQ
Speaker presentations and a recording of the workshop will be available shortly after the workshop.

For any questions or comments during the workshop, please email: sec-cert@nist.gov or send us a tweet at:

@usNISTgov #CUIsecurity

Registration Contact:
Pauline Truong
NIST Conference Services
pauline.truong@nist.gov
301-975-3258

Technical Contact:
Victoria Yan Pillitteri
NIST Computer Security Division
vyan@nist.gov
301-975-8542

Continuing Education Units (CEUs): Attendees are always welcome to self-report to their authoritative certification bodies to request CEUs for attending this event.

Resources

NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and supplemental materials are available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, and supplemental materials are available at: https://csrc.nist.gov/publications/detail/sp/800-171a/final

Information about the Controlled Unclassified Information (CUI) Program is available at: https://www.archives.gov/cui