# Meet our panelists

**Fred Jones**
**RTX**

Fred Jones is a Senior Technical Fellow with RTX Technology Research Center. He has 24 years of experience in the Aerospace Defense Industry, with the past 10 years focused on leading Cyber Offensive and Defensive R&D programs. Prior to joining the research center, he was the Cyber Technology Area Director for Raytheon and an embedded systems software developer. His patents and trade secrets are in the areas of Anti-Fragile Software Systems, Zero Trust Endpoint Network Security, Integrating FPGAs into Digital Twins, and Software Assurance with Digital Twins.

**Richard (Rich) Massey (CISSP)**
**Boeing**

Rich is a Boeing Senior Tech Fellow. He is responsible for Product Security Engineering Technical Excellence across the Boeing enterprise. Rich's primary focus and vision is to ensure the security and resiliency of our products and services to the aerospace community. Rich serves as the Chairman for the DoD Cyber Industry Technical Advisory Working Group. He supports the NDIA System Security Engineering Committee and Open Management Systems Security Working Groups.
Rich has over 35 years' experience with avionics developments for USAF, USN and Army Aviation. Rich has been responsible for the development and integration of avionics architectures, avionics and support equipment. His background includes mission processing, displays, recorders, sensors and both traditional networking and avionics busses. Rich has successfully integrated security into advanced systems architectures and avionics. Rich has a MSEE from Washington University St Louis, and a BSEE from Rose-Hulman Institute of Technology.

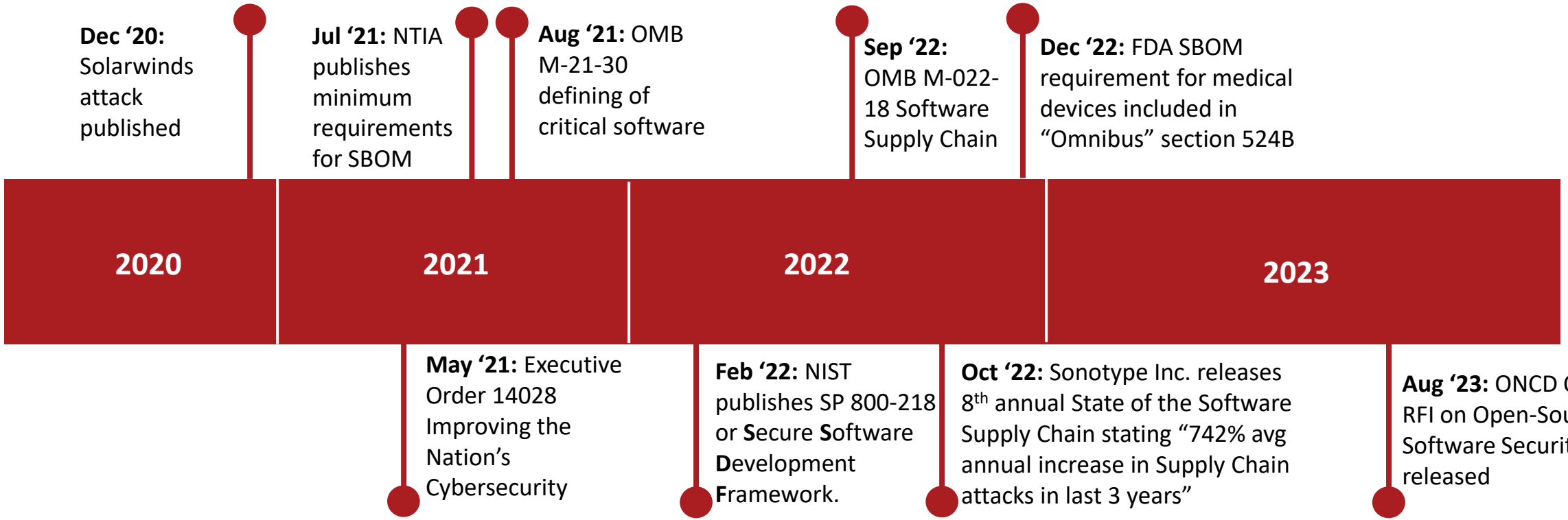
**Dr. Ronda Henning**
**L3Harris**

Senior Fellow, Chief Technologist, L3HarrisTechnologies. Ms. Henning is the Senior Information Systems Security Engineer in L3Harris Technologies. In this position she is responsible for advanced system architectures across the Harris customer communities.
Over her 30+ years at L3Harris, Ms. Henning has served as the security architect of various L3Harris programs. These include space and terrestrial networks, advanced DARPA concepts, and various research programs.
Dr. Henning has a Ph.D. in Information Assurance from Nova Southeastern University, an M.B.A. from the Florida Institute of Technology, an M.S. from the Johns Hopkins University, and a B.A. from the University of Pittsburgh. She holds several security certifications including the CISM and CISSP. Dr. Henning holds 6 patents in security visualization and situational awareness.

**Moderator: Kirk Rasmussen - RTX**

Kirk Rasmussen is a Technical Fellow with Raytheon, an RTX Business, specializing in Cybersecurity technical innovation. Throughout Kirk's 27 years in IT/DT, 19 at RTX, he has led architecture development of large-scale IT infrastructures across internal, and USG programs. For the last 5 years has been leading the secure open-source software enablement for RTX. Kirk has a B.S. in MIS from Iowa State University and holds numerous certifications including: RTX Certified Architect, GCCC, GSEC.

# Timeline of Events

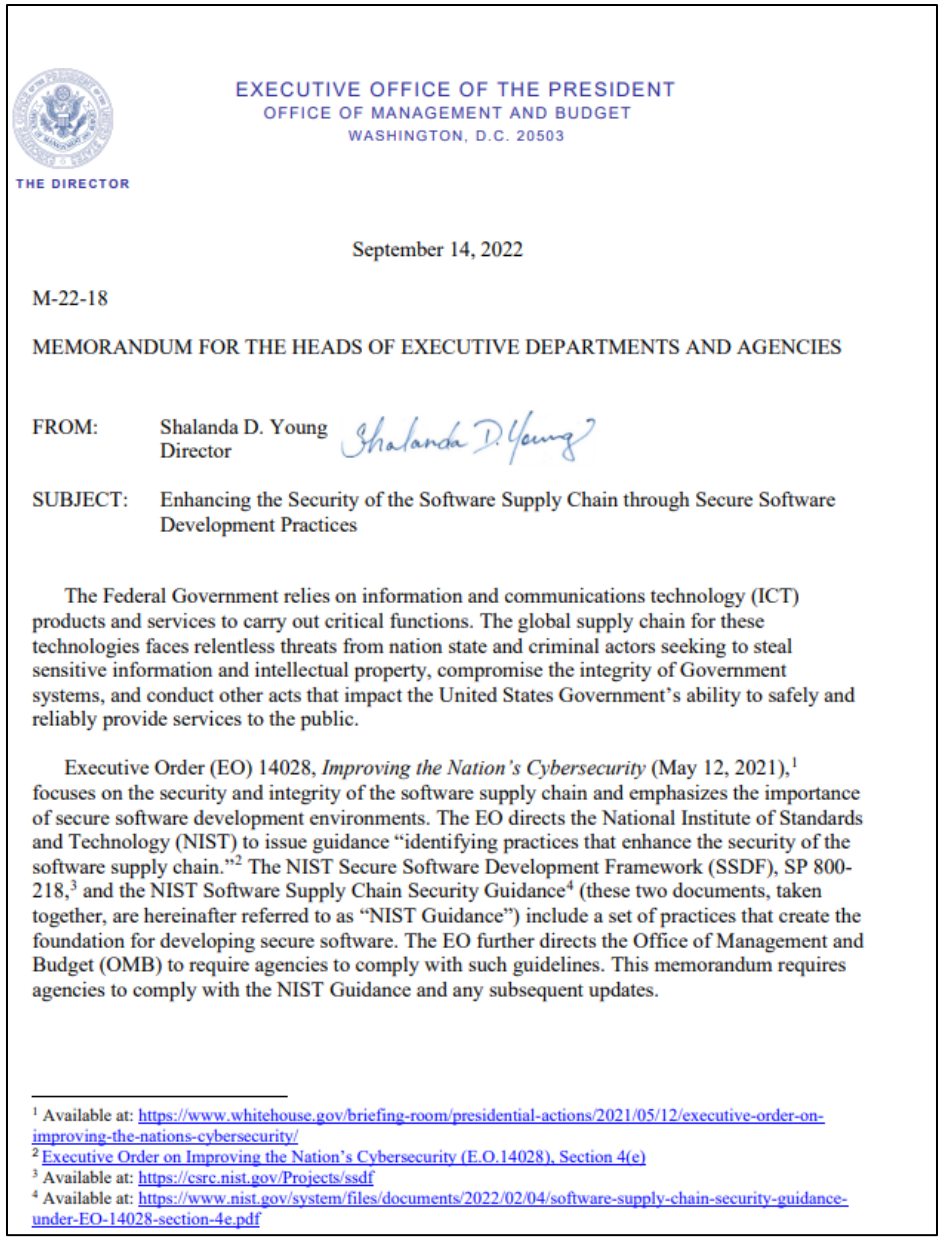


# Contents of OMB Memo

- **Apply to…software developed after the effective date…as well as…existing software that is modified…after the effective date of this memorandum.**

- **Agencies required to obtain self-attestation from software producer before using the software**
  - Includes all 3rd party libraries
  - Minimum content of attestation letter
  - If FOSS, perform assessment via 3PAO per FedRAMP

- **Agencies may obtain artifacts that demonstrate conformance as needed**
  - References multiple potential artifacts with SBOMs being the flagship



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government's ability to safely and reliably provide services to the public.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain."[2] The NIST Secure Software Development Framework (SSDF), SP 800-218,[3] and the NIST Software Supply Chain Security Guidance[4] (these two documents, taken together, are hereinafter referred to as "NIST Guidance") include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] Executive Order on Improving the Nation's Cybersecurity (E.O.14028), Section 4(e)
[3] Available at: https://csrc.nist.gov/Projects/ssdf
[4] Available at: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

# Contents NIST 800-218

- **Risk Based Framework…not process…not specification…not procedure; risk that customers will implement as compliance**
  - "The SSDF does not prescribe how to implement each practice."
  - "The SSDF defines only a high-level subset of what organizations may need to do…"
  - "Not all practices are applicable to all use cases; organizations should adopt a risk-based approach to determine what practices are relevant, appropriate, and effective to mitigate the threats to their software development practices."
  - "The intention of the SSDF is not to create a checklist to follow, but to provide a basis for planning and implementing a risk-based approach to adopting secure software development practices."

Prepare the Organization

Protect the Software

Produce Well-Secured Software

Respond to Vulnerabilities