RMF 2.0

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

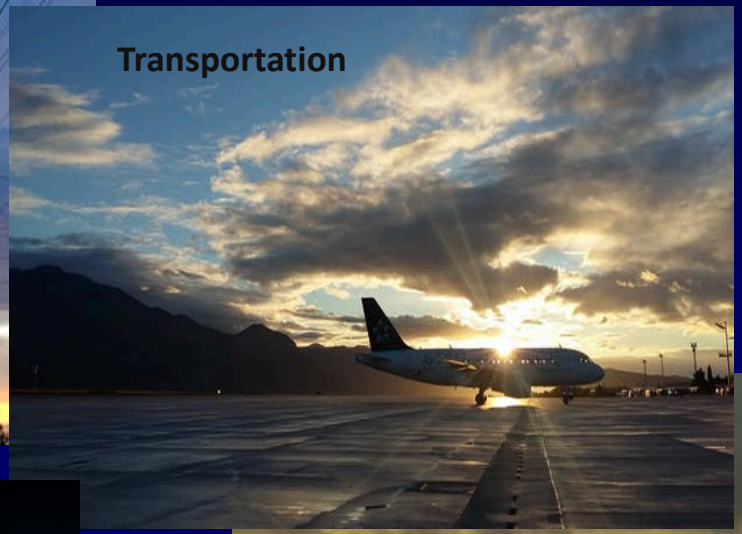
Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

The Current Landscape.

It's a dangerous world in cyberspace…

Risk.

Function (threat, vulnerability, impact, likelihood)



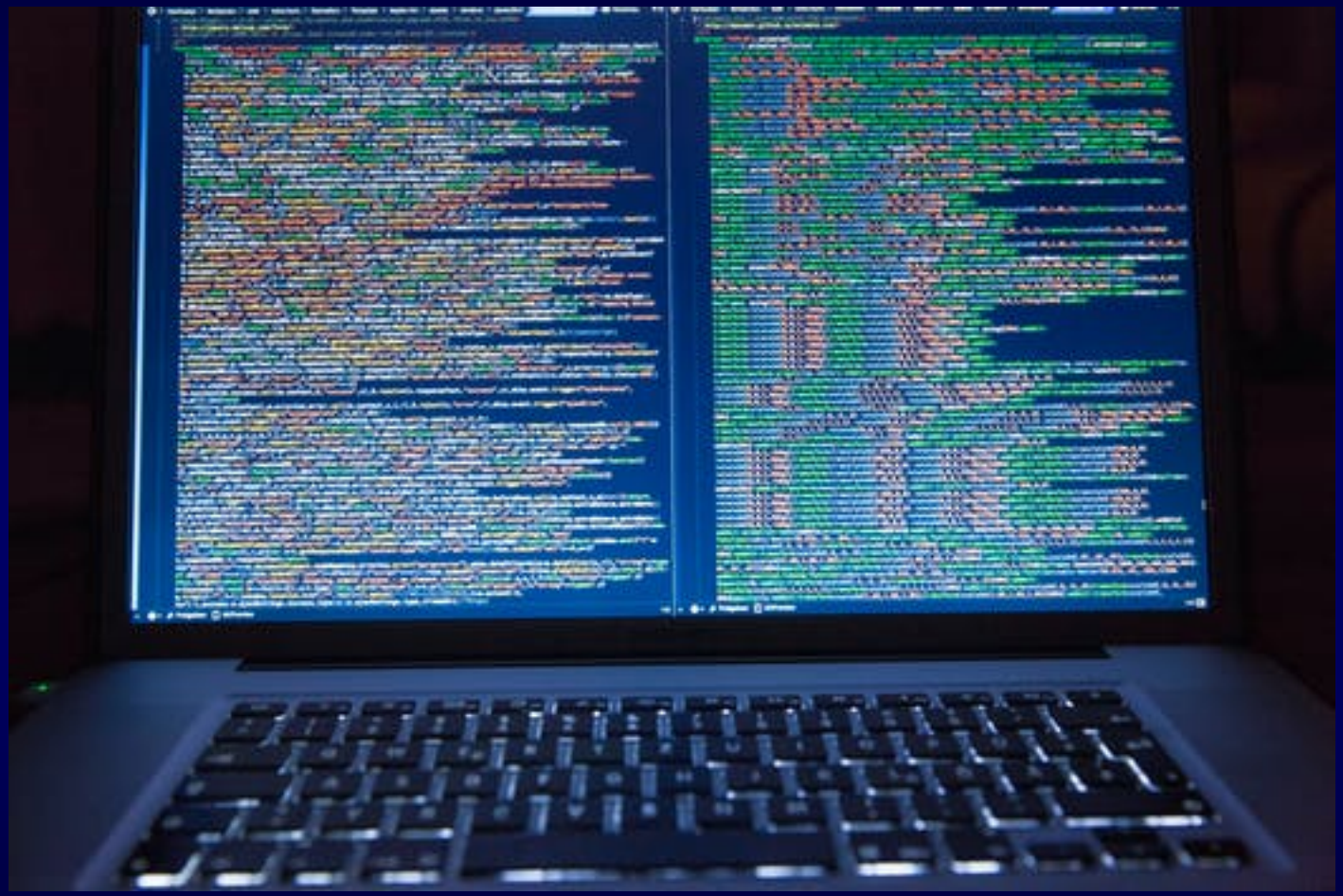
- Resilient Military Systems and the Advanced Cyber Threat
  - Cyber Supply Chain
    - Cyber Deterrence

Defense Science Board Reports

Complexity.

Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Data. Data. Everywhere.



Houston, we have a problem.

Protecting critical systems and assets—

The highest priority for the national and economic security interests of the United States.


Defending cyberspace
in 2018 and beyond.

Federal Government's Modernization Strategy

- Identify and develop federal shared services.
- Move to FedRAMP-approved cloud services.
- Isolate and strengthen protection for high value assets.

Reduce and manage the complexity of systems and networks…
Engineering more trustworthy, secure, and resilient solutions.

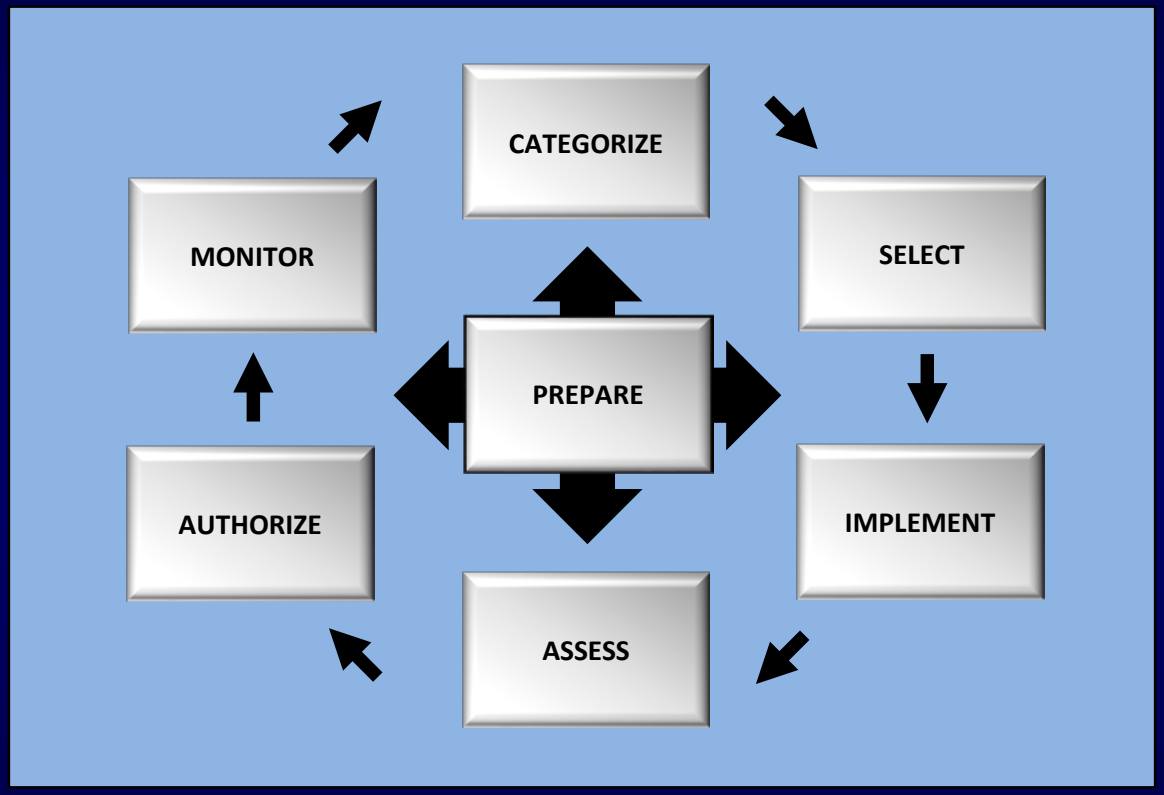
Simplify. Innovate. Automate.

- NIST SP 800-37, Revision 2

  Risk Management Framework for Information Systems and Organizations

  A System Life Cycle Approach for Security and Privacy

Risk Management Framework (RMF) 2.0



RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 1

To provide closer linkage and communication between the risk management processes and activities at the C-suite or governance level of the organization and the individuals, processes, and activities at the system and operational level of the organization.

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 2

To institutionalize critical enterprise-wide risk management preparatory activities to facilitate a more effective, efficient, and cost-effective execution of the RMF.

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 3

To demonstrate how the Cybersecurity Framework can be aligned with the RMF and implemented using established NIST risk management processes.

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 4

To integrate privacy risk management concepts and principles into the RMF and support the use of the consolidated security and privacy control catalog in NIST Special Publication 800-53, Revision 5.

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 5

To promote the development of trustworthy secure software and systems by aligning life cycle-based systems engineering processes in NIST Special Publication 800-160 with the steps in the RMF.

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 6

To integrate supply chain risk management (SCRM) concepts into the RMF to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC.

RMF

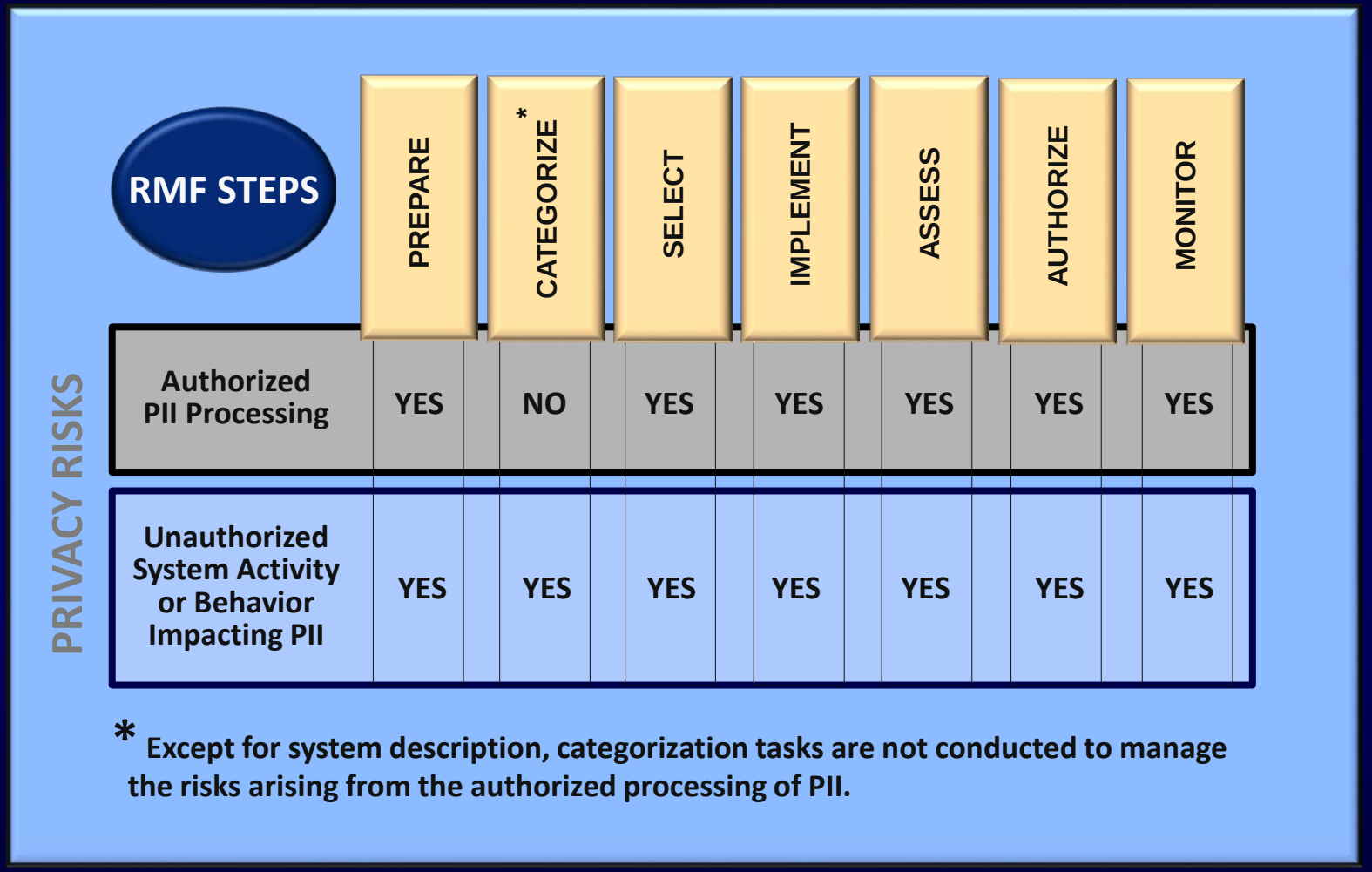
RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

OBJECTIVE 7

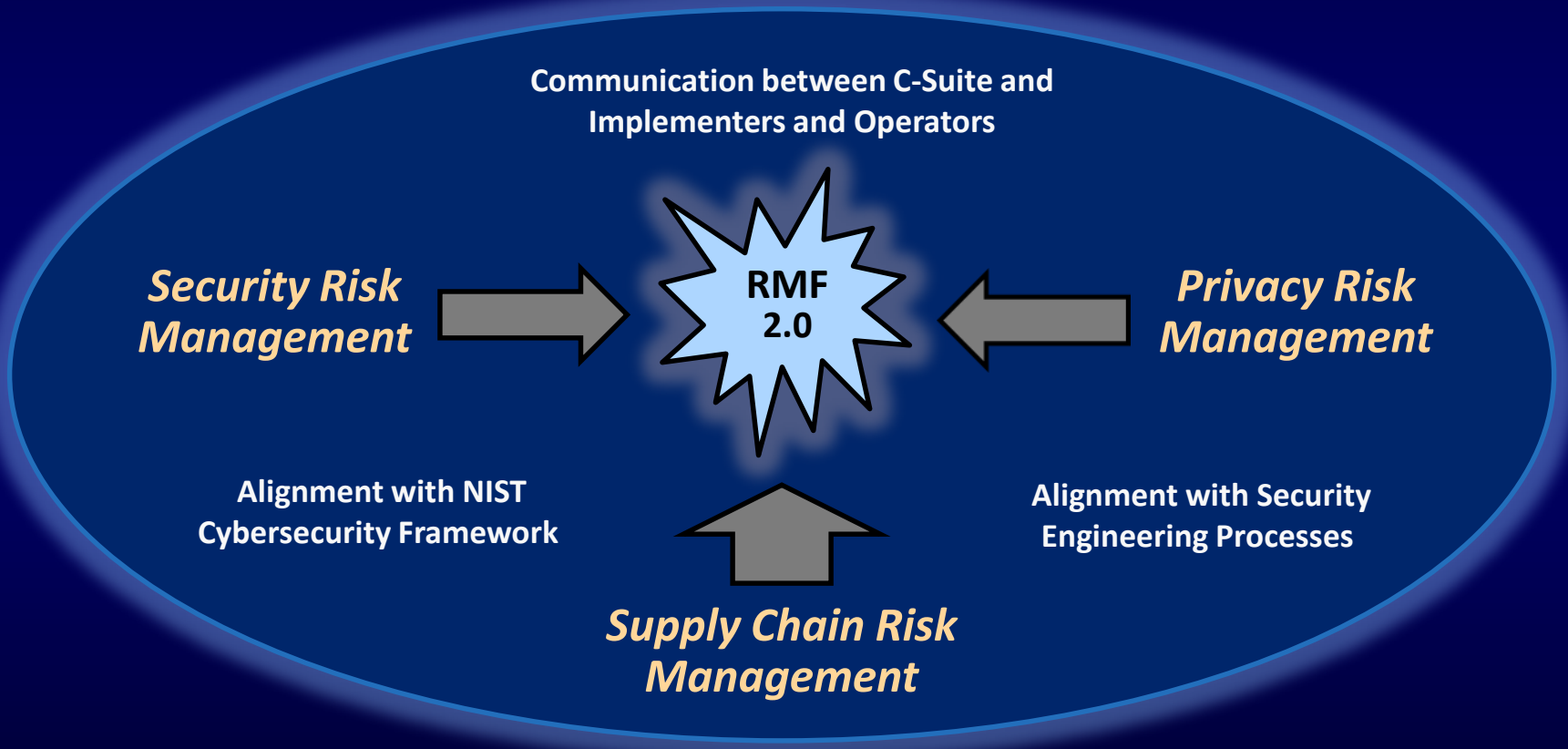
To provide an alternative organization-generated control selection approach to complement the baseline control selection approach.

Security and Privacy.



* Except for system description, categorization tasks are not conducted to manage the risks arising from the authorized processing of PII.

A unified framework for managing security, privacy, and supply chain risks.



Everything (good or bad) that happens with the RMF starts at the top of the organization.

Prepare Step

Organization Level

Preparing organizations to execute the RMF from the enterprise perspective…

Outcomes

- Individuals are identified and assigned key roles for executing the RMF.

  [*Cybersecurity Framework:* **ID.AM-6**; **ID.GV-2**]

- A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.

  [*Cybersecurity Framework:* **ID.RM**]

- An organization-wide risk assessment is completed or an existing risk assessment is updated.

  [*Cybersecurity Framework:* **ID.RA**]

- Tailored control baselines for enterprise-wide use are established and made available.

  [*Cybersecurity Framework:* **Profile**]

Prepare Step

Organization Level

Preparing organizations to execute the RMF from the enterprise perspective…

Outcomes

- Common controls that are available for inheritance by organizational systems are identified, documented, and published.

  [*Cybersecurity Framework:* **No mapping**]

- A prioritization of organizational systems with the same impact level is conducted.

  [*Cybersecurity Framework:* **ID.AM-5**]

- An organization-wide strategy for monitoring control effectiveness is developed and implemented.

  [*Cybersecurity Framework:* **DE.CM**]

Prepare Step

System Level

Preparing organizations to execute the RMF from the system perspective…

Outcomes

- Missions, business functions, and processes the system is intended to support are identified.
  [*Cybersecurity Framework:* **Profile; Implementation Tiers; ID.BE**]
- The stakeholders having an interest in the system are identified.
  [*Cybersecurity Framework:* **ID.AM; ID.BE**]
- Stakeholder assets are identified and prioritized.
  [*Cybersecurity Framework:* **ID.AM**]
- The authorization boundary (system-of-interest) is determined.
  [*Cybersecurity Framework:* **No mapping**]
- The types of information processed, stored, and transmitted by the system are identified.
  [*Cybersecurity Framework:* **ID.AM-5**]

Prepare Step

System Level

Preparing organizations to execute the RMF from the system perspective…

Outcomes

- For systems that process PII, the information life cycle is identified.

  [*Cybersecurity Framework:* **No mapping**]

- A system-level risk assessment is completed or an existing risk assessment is updated.

  [*Cybersecurity Framework:* **ID.RA**]

- Protection needs and security and privacy requirements are defined and prioritized.

  [*Cybersecurity Framework:* **ID.GV; PR.IP**]

- The placement of the system within the enterprise architecture is determined.

  [*Cybersecurity Framework:* **No mapping**]

- The system is registered for management, accountability, coordination, and oversight.

  [*Cybersecurity Framework:* **ID.GV**]

Life Cycle Security and Privacy

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal

Build It In…

Transparency.

Traceability.

Trust.

On the Horizon…

- NIST Special Publication 800-37, Revision 2
  Risk Management Framework for Information Systems and Organizations
  Final Publication: October 2018
- NIST Special Publication 800-53, Revision 5
  Security and Privacy Controls for Information Systems and Organizations
  Final Publication: December 2018
- NIST Special Publication 800-53A, Revision 5
  Assessing Security and Privacy Controls in Information Systems and Organizations
  Final Publication: September 2019

Some final thoughts.

Work smarter, not harder.

Institutionalize.

The ultimate objective for security.

Operationalize.

Leadership.
Governance.
Accountability.

Government

Academia

Security is a team sport.

Industry

Security. Privacy. Freedom.


Federal Computer Security Managers' Forum
Offsite Meeting
May 15-16, 2018
NIST Gaithersburg (MD) Campus
Registration closes May 10, 2018
For more information, the agenda, and to register:
https://go.usa.gov/xQYFe
Please send questions to sec-forum@nist.gov

RMF

RISK MANAGEMENT FRAMEWORK

SIMPLIFY. INNOVATE. AUTOMATE.

Ron Ross

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Email
ron.ross@nist.gov

Mobile
301.651.5083

LinkedIn
www.linkedin.com/in/ronross-cybersecurity

Twitter
@ronrossecure

Web
csrc.nist.gov

Comments
sec-cert@nist.gov