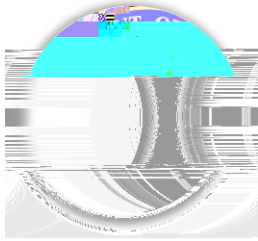


RMF for HPC and RDT&E

NIST / NRF HPC Security Working Group

Rickey Gregg

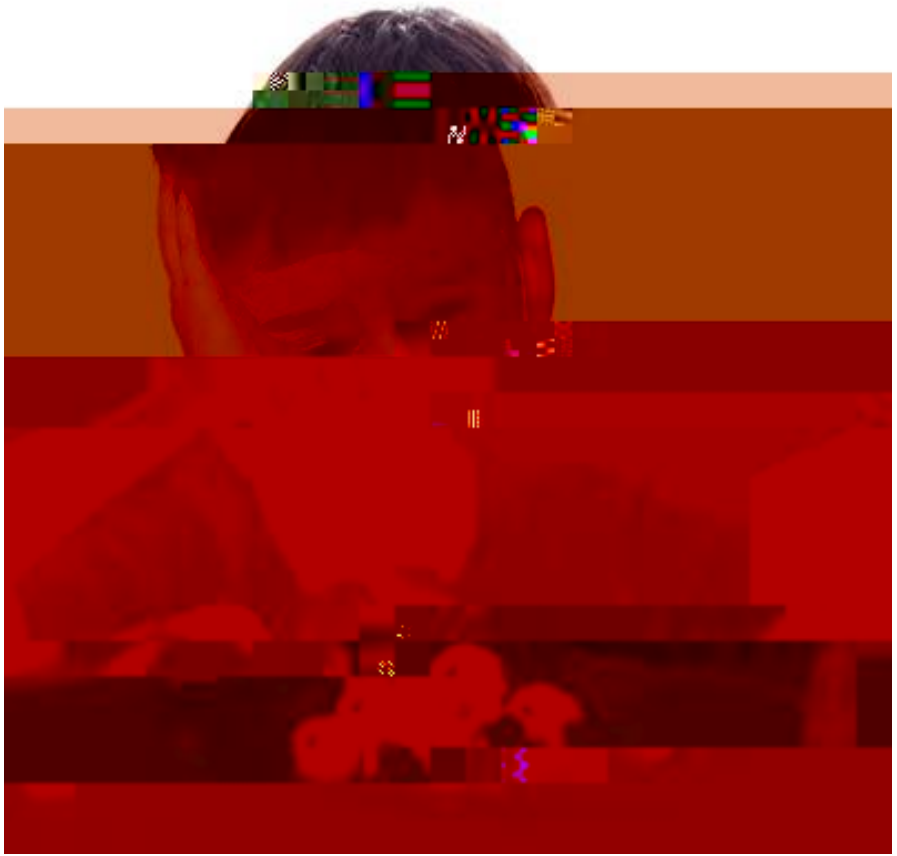
20 May 2024

Cybersecurity is like Herding Cats

RMF & RDT&E

Go together like peanut butter and jelly…

Choosing an RMF Package Type…



RMF Package Types

Interim Authority to Test (IATT) – *6 to 12 months*

– Temporary systems for test events or proof of concept

Assess Only – *12 months*

– Introducing new systems into an existing authorized enclave or system

Technology Insertion, new HPC, new major applications

Authority to Connect (ATC) – *Up to 3 years or ATD*

– When incorporating an existing authorized system/software into an enclave

ACAS, HBSS, software developed/tested by external entity and accepted via reciprocity

Assess and Authorize (A & A) – *3 years*

– Authorizing new or existing enclaves or systems

Software rollout, data center, storage array

Inheriting Controls

Inheritance offers time savings by incorporating security control test results from an entity that has previously obtained approval.

Inheritable Controls

Controls can be inherited from a variety of sources.

- ***Tier I*** *(High level organization)*
  - *DoD, DoE via a Common Control Provider (CCP)*
  - *Full inheritance*

- ***Tier II*** *(Mission or business processes)*
  - *Common Control Provider or host organizational package*
  - *Full inheritance*

- ***Tier III*** *(System or user level)*
  - *Cybersecurity Service Provider (CSSP)*
  - *User organization*
  - *Hybrid inheritance*

**** NOTE ****

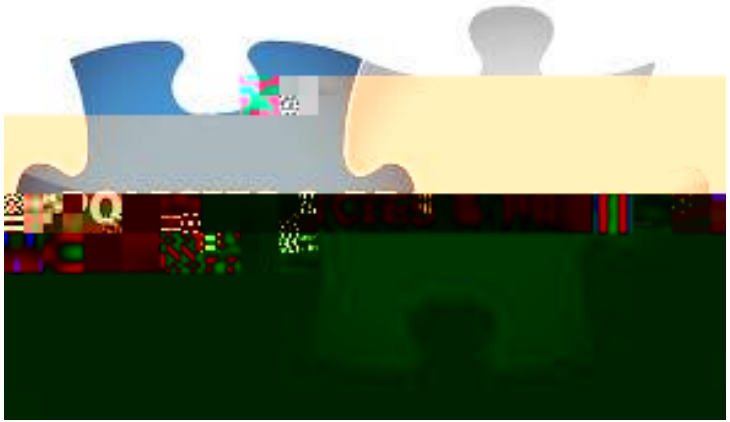
Hybrid inheritance = each side has responsibilities for the compliance of the security control.

Reciprocity

Reciprocity goes hand in hand with inheritance.

-
  and the associated costs in time and resources. *Knowledge Service)*
- Inheritance focuses on the controls; reciprocity is aimed at valid approvals of the system or software.
-

Policies & Procedures



Policies & Procedures - DoD

Non-DoD Policies

Other federal organizations, industry partners and academia generally follow NIST guidance

- SP800-18 Developing Security Plans
- SP800-30 Conducting Risk Assessments
- SP800-37 Risk management Framework
- SP800-39 Managing Information Security Risk
- SP800-53 Security & Privacy Controls
- SP800-53A Assess Security & Privacy Controls
- SP800-137 Information System Continuous Monitoring
- SP800-160 Systems Security Engineering
- SP800-223 High Performance Computing Security
- FIPS 199 Security Categorization

NIST & DoD guidance are derived from higher level documents

- Appendix III to OMB Circular A-130, Security of Federal Automated Information Resources
- Public Law 100-235, Computer Security Act of 1987
- Executive Orders

Questions?

Rickey Gregg
HPCMP Cybersecurity PM
rickey.gregg@dren.hpc.mil

Abbreviations and Acronyms

TERM	DEFINITION
A & A	Assess and Authorize
AO	Authorizing Official
ATC	Authority to Connect
CIA	Confidentiality, Integrity, Availability
CSSP	Cybersecurity Service Provider
DISA	Defense Information System Agency
DREN	