RMF for HPC and RDT&E
NIST / NRF HPC Security Working Group
Cybersecurity is like Herding Cats
Outline

• Risk Management Framework Overview
  – RMF & RDT&E
  – RMF Package Types
  – Inheritance
  – Reciprocity

• Policies & Procedures
  – NIST
  – DoD Guidance

• Questions
RMF & RDT&E

Go together like peanut butter and jelly…
RMF

RMF addresses three basic security principles: **Confidentiality**, **Integrity**, & **Availability** (CIA) to ensure that data cannot be shared or accessed without authorization, cannot be accidentally or maliciously changed, and is available to authorized personnel when and where needed.

RMF provides consistency for implementing new systems and a mechanism to evaluate risk
- Documentation, configuration settings, vulnerability scanning, reviews and tiered approvals

Processes can be adjusted to fit unique systems
- Package types and approval durations
RMF Has Seven Steps ;)

1. Prepare
2. Categorize
3. Select
4. Implement
5. Assess
6. Authorize
7. Monitor
RMF & RDT&E

Most RMF efforts are focused on the product or result; e.g., software, hardware, system, facility.

- The focus in RDT&E environments should be on the process.
  - How do we develop the software or code? How do we build these systems or appliances? How do we accomplish the test?

- By shifting the focus to the process, we allow for greater flexibility of what needs to be authorized and how to identify and assess the risk.
  - Focus on the HOW, not the WHAT…
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
RMF Inheritance can be nice…
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.
  
  - “reduce redundant testing assessing and documentation, and the associated costs in time and resources.” *(RMF Knowledge Service)*
  
  - Inheritance focuses on the controls; reciprocity is aimed at valid approvals of the system or software.
  
  - Reciprocity can vary from organization to organization, ultimately the decision to accept another entity’s approval resides with the Authorization Official (AO), the individual accepting risk for the system or software.
  
  - "I expect testing re-use and reciprocity to be implemented except when the cybersecurity risk is too great." *(Dep Defense Secretary, K. Hicks)*
Policies & Procedures
Policies & Procedures - DoD

- The HPCMP adheres to DoD Instructions, Regulations and Memorandums
  - 8500.01 Cybersecurity
  - 8510.1 Risk Management Framework
  - Defense Information System Agency (DISA)
    - Security Technical Implementation Guides (STIGs)

- DoD guidance is 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

- HPCMP Polices and Memos derived from mandated documents
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

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>A &amp; A</td>
<td>Assess and Authorize</td>
</tr>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>ATC</td>
<td>Authority to Connect</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity, Availability</td>
</tr>
<tr>
<td>CSSP</td>
<td>Cybersecurity Service Provider</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information System Agency</td>
</tr>
<tr>
<td>DREN</td>
<td>Defense Research and Engineering Network</td>
</tr>
<tr>
<td>eMASS</td>
<td>Enterprise Mission Assurance Security System</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>IATT</td>
<td>Interim Authority to Test</td>
</tr>
<tr>
<td>ISSM</td>
<td>Information System Security Manager</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>RDT&amp;E</td>
<td>Research Development Test &amp; Evaluation</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Control Assessor</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication (NIST naming convention)</td>
</tr>
<tr>
<td>STIG</td>
<td>Security Technical Implementation Guide</td>
</tr>
</tbody>
</table>