



Implement the New NIST RMF Standards and Meet the 2023/2024 FISMA Metrics

September 20-21, 2023 · Online Virtual Class

AGENDA

Day 1: Wednesday, September 20, 2023

- 8:00AM **Seminar Overview and Introductions**
Resources, Goals, Objectives
Group Introduction Breakouts
- 8:50AM Break
- 9:00AM **FISMA: Process, Players, Frameworks, and New Requirements**
2023 FISMA Process
 - President's Executive Order 14028
 - OMB Memos and Directives – 2023 FISMA Guidance, Privacy Reporting and On-Going Authorization, A-130
 - Zero-Trust Architecture – SP800-207
 - DHS Binding Operational Directives (BODs) and Emergency Directives (EDs)**Frameworks**
 - Risk Management Framework (RMF) – SP800-37
 - Cybersecurity Framework (CSF) – NIST CSF
 - System Development Lifecycle (SDLC) – SP800-64
 - System Security Engineer Framework (SSEF) – SP800-160
 - High Value Assets (HVA) Frameworks – OMB M-17-09
- 9:50AM Break
- 10:00AM **NIST Special Publications Update**
Guest Speaker: Jeremy Licata, CISSP, Information Security Specialist, National Institute of Standards and Technology (NIST)
- 10:50AM Break
- 11:00AM **RMF Preparation: Roles and Authorization Boundary Identification**
Authorization Boundary Characteristics
System's Categorization Exercise
Examples of Real-World System's Boundaries
Group Authorization Boundary Identification Breakouts
- 12:00AM Lunch
- 1:00PM **RMF Categorization: System Categorization**

Risk Modeling: Quantitative, Qualitative, and Hybrid – SP800-30/SP800-39

System's Categorization Exercise

Categorization Processes – FIPS-199/SP800-60

System Maximum Impact Level – SP800-30/SP800-39/SP800-60

Examples of Real-World System's Categorizations

Group System's Categorization Breakouts

1:50PM Break

2:00PM DHS Cybersecurity Initiatives Update

Guest Speaker: Fabion (Frank) Husson, CISSP, *Insights Branch Chief, Cyber Security Division (CSD), U.S. Department of Homeland Security (DHS) is invited to speak on this topic.*

2:50PM Break

3:00PM **RMF Select:** Baseline Controls, Control Types, and Leveraging the Enterprise Solutions

Security Control Baseline/Best Practices – FIPS 200/SP800-53/SP800-53B

Assurance and Trust

System Specific, Common, Hybrid, Core Controls

Group System Control Type Identification Breakout

4:00PM Adjourn



Implement the New NIST RMF Standards and Meet the 2023/2024 FISMA Metrics

September 20-21, 2023 · Online Virtual Class

AGENDA

Day 2: Thursday, September 21, 2023

- 8:00AM **RMF Implementation:** Tailoring Controls and Compensating Controls
- Baseline Assumptions and National Security Systems – SP800-53/CNSSI-1253
 - Tailoring Controls – Risk-Based and Cost-Effective
 - Group Control Tailoring Breakouts**
 - Compensating Controls – Operations and Risk Reducing
 - Group Compensating Control Breakouts**
- 8:50AM Break
- 9:00AM **RMF System Documentation:** System Security Plan, Overlays and Consolidated Plans
- Plan Requirements, Outlines, and Potential Consolidations**
 - Operations Manual and System Security Plan (SSP) – SP800-18
 - Security-focused Configuration Management Plan (SecCMP) – SP800-128
 - Patch Management Plan (PMP) – SP800-40
 - Information Security Control Monitoring Plan (ISCMP) – SP800-137
 - Incident Response Plan (IRP) – SP800-61/SP800-83
 - Contingency Plan (CP) – SP800-34
 - Cybersecurity Framework and Privacy Control Framework.....
 - Free Overlays and Templates
- 9:50AM Break
- 10:00AM **RMF Assess and Authorization:** Risk Assessments Methods, Expertise and Mitigations
- Assessments – Requirement, Expertise, and Options
 - Authorizations – For Systems, For Common Controls, and For Use
 - Authorization Exercise**
- 10:50AM Break
- 11:00AM **Ongoing Authorizations:** Automation and Near-Time Situational Security Awareness
- Security Automation Domains
 - Leveraging Automation and Services
 - Security Content Automation Protocol (SCAP)
 - DoD Host-Based Security System (HBSS) Solutions
 - Assured Compliance Assessment Solution (ACAS)
 - Continuous Diagnostics and Mitigation (CDM) Program
 - Continuous Monitoring Dashboard
 - Bonding Operational Directives (BOD), EINSTEIN, Trusted Internet Connection (TIC), Managed Trusted Internet Protocol Services (MTIPS), and DHS Cybersecurity Hygiene Reviews

- 12:00PM Lunch
- 1:00PM **RMF Monitoring:** Continuous Monitoring and Monitoring Frequencies
Information Continuous Monitoring Programs
Endpoint Detection and Response (EDR)
Monitoring Frequency for Controls Exercise
- 1:50PM Break
- 2:00PM **Respond and Recovery:** Incident Response and Contingency Planning
Incident Response
Cybersecurity Incident & Vulnerability Response Playbooks
Contingency Planning
- 2:50PM Break
- 3:00PM **Cybersecurity Future:** Clouds, Online Services, Teleworking and AI
Clouds – Types and Authorizations
Internet – Teleworking and Online Services
Savings – Travel, Contingency Options.....
- 3:50PM Summary
- 4:00PM Adjourn

Note: Many products will be identified but identifying them is not an endorsement.