



NS2022

ACCELERATING INNOVATION

Working with Federal Government and US DOD Customers

*Moderator: David Hornosky
Tuesday 5 April 2022*



Purpose

The DOD and other governmental agencies continue to enhance their security and operational requirements. This session will give you an overview of the latest government security requirements as well as how System's Integrators, General Contractors, and independent testing agencies are working successfully with the government on upgrades, new deployments, and the future of cybersecurity in this space.

Panelists



David Hornosky

Session owner and moderator



Global Strategy Leader- Government and Defense



Owen Green



Senior Systems Engineer (Spectrum
Madison, AL



Jacob Jackson



Project Manager (Dewberry Design

Charlotte, NC (by way of Germany)



Austin Coots



Cyber Projects Manager (Aleta Technologies,
Huntsville, AL



Bill Smith



Lead Software Architect (Tridium,



Discussion



DIACAP → RMF



DIACAP= DOD Information Certification and Assurance Process
RMF=Risk Management Framework

Risk Management Framework (DME)

Risk Management Framework: step by step



Prepare
formal risk
management
strategy



Categorize
identified
risks



Select
security
controls



Implement
selected
security
controls



Assess
efficacy of
security
controls



Authorize
continued use
of security
controls



Monitor
security
controls
frequently

Niagara 4 Artifacts for RMF

Name

 01-Access Control
 02-Awareness and Training
 03-Audit and Accountability
 04-Configuration Management
 05-Contingency Planning
 06-Identification and Authentication
 07-Incident Response Plan
 08-Maintenance Procedures
 09-Media Protection
 10-Physical and Environmental Security
 11-Program Management and Planning
 12-Personnel Security
 13-Risk and Security Assessment
 14-Systems and Services
 15-System and Communications Protecti...
 16-System and Information Integrity
 17-CONOPS_Niagara



NS2022

ACCELERATING INNOVATION

CHARLOTTE, NC | APRIL 4-6

Q&A

Thank you!

