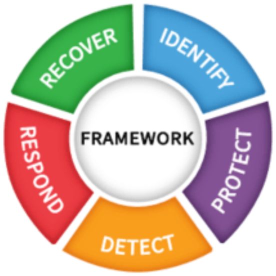
2020
FAA CYBERSECURITY AWARENESS SYMPOSIUM
THEME – "CYBER HYGIENE"

CYBER ENTERPRISE ARCHITECTURE

Mission

Provide strategic and tactical analysis of new technologies and overarching systematic approaches, which shapes the evolution of Air Traffic Organization (ATO) Systems and Services.

Cybersecurity Framework (CSF)

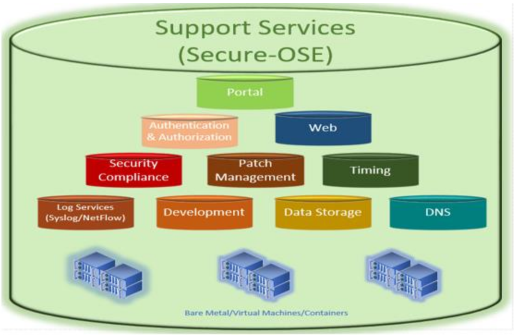


- Research and tailor framework
- Describe current security posture
- Describe target security posture
- Identify risks, issues, and opportunities
- Communicate and assess annually

Unmanned Aircraft Systems (UAS)

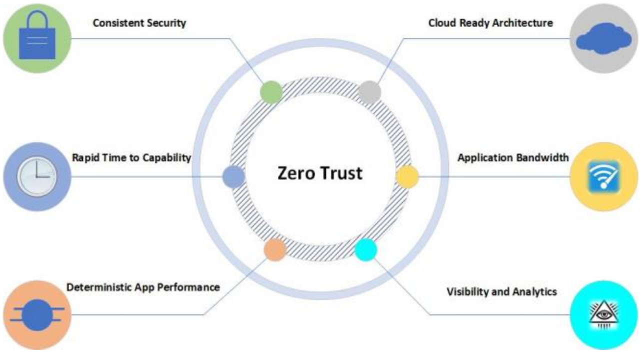
- Collaborate with internal and external stakeholders, advising on best practices relevant to Cybersecurity
- Establishment of domestic and international Policy, Strategic Plans, best practices, and Roadmaps
- Proactively track UAS cybersecurity issues and how UAS and C-UAS integration in the NAS may impact safety of the NAS and FAA Systems
- Identify emerging and integration needs for UAS and Counter UAS (C-UAS)

Secure Operational Support Environment (Secure-OSE)



- An Enterprise approach, Proactive vs. Reactive, improving security compliance and posture
- Common security controls and objectives for NAS Services and improves operations and service efficiency
- Characterizes risk and streamlines remediation
- Combines software development with security for integration into operational environments

Zero Trust Architecture



- All data sources and computing services are considered resources and access to resources is by dynamic policy
- The enterprise collects as much information as possible about the current state of the network infrastructure which is used to mitigate risk and improve posture
- All communication is secured regardless of location
- Authentication and authorization are dynamic and strictly enforced before allowing access to resources