2020 FAA Cybersecurity Awareness Symposium
Securing the Aviation Ecosystem | "Cyber Hygiene"

Cyber Enterprise Architecture

Date: October 20, 2020

Federal Aviation Administration

Cyber Enterprise Architecture

Mission Statement

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

Functional Areas

Enterprise & System Architectures

Unmanned Aircraft System (UAS)

International Aviation Trust Framework (IATF)

Secure Operational Support Environment (Secure-OSE)
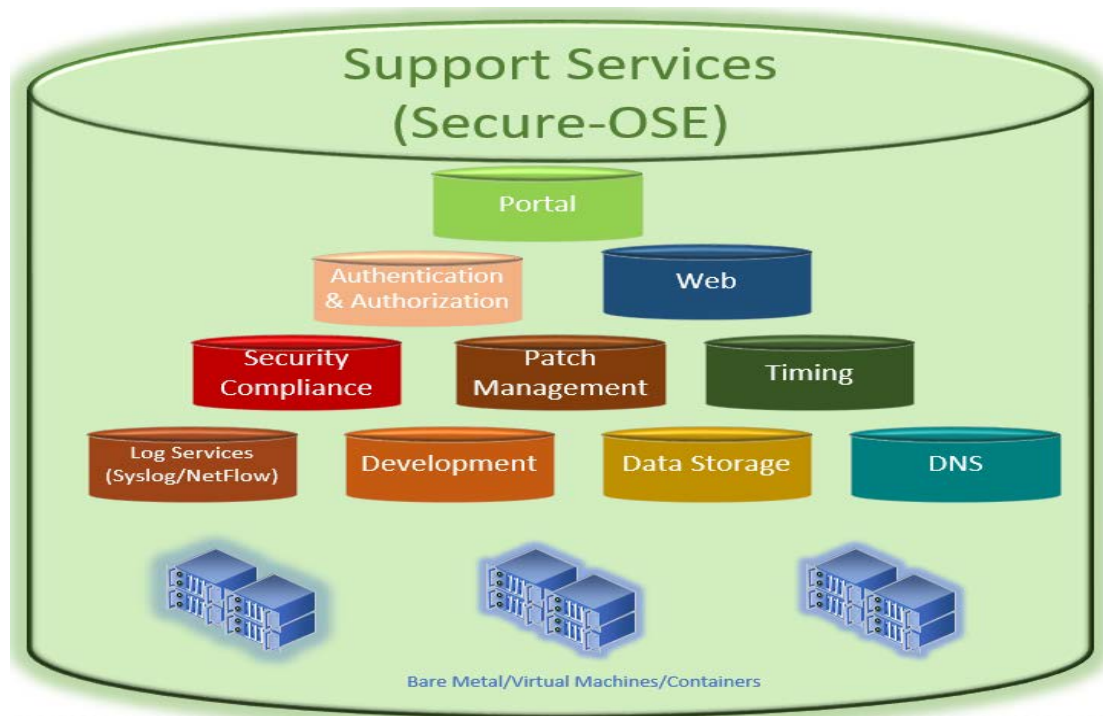
Cybersecurity Framework (CSF)

Strategic Plans

Roadmaps

Commercial Space

Supply Chain Risk Management (SCRM)

Secure Operational Support Environment (Secure-OSE)

- An Enterprise approach, Proactive vs. Reactive, improving security compliance
- Common security controls and objectives for NAS Services
- Improves upon Operations and Service efficiency
- Characterizes risk and streamlines remediation

Zero Trust Architecture
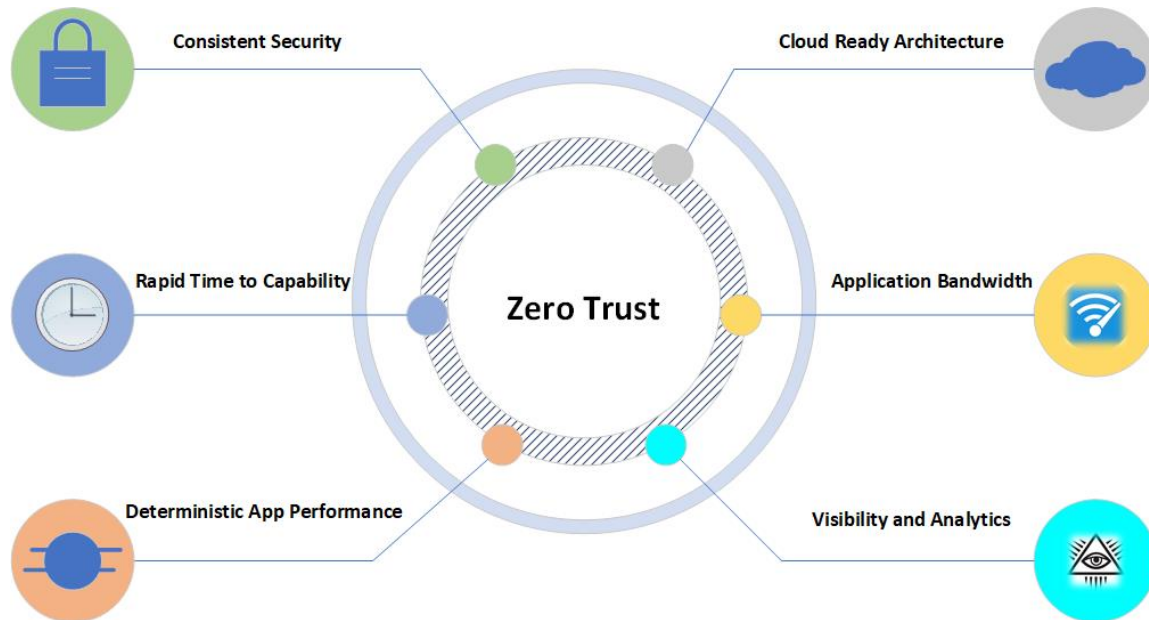
- All Data Sources and Services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy
- The Enterprise ensures all owned and associated devices are in the most secure state possible and monitored to ensure they stay that way
- Resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of the network infrastructure which is used to mitigate risk

Unmanned Aircraft Systems (UAS)

- Collaborate with internal and external stakeholders, advising on best practices relevant to Cybersecurity
- Track UAS cybersecurity issues and how UAS integration may impact the safety of FAA systems
- Review and participate in development of international standards assuring FAA interests
- Identify emerging and integration needs for UAS and Counter UAS (C-UAS)
- Establishment of Policy, Strategic Plans, and Roadmaps

Cybersecurity Framework (CSF)

ACG reviews new
- FAA policies,
- Public laws/policies,
- NIST guidance,
- Best practices,
- New threats,
- Audit results,
- Recent cyber incidents.

The ATO Cybersecurity Strategic Plan and ACG Budget Requests incorporate the prioritized mitigations for necessary areas of improvement.

Research and tailor framework.

Communicate and assess annually.

Describe current security posture.

Assess current security posture, based on POA&Ms and qualitative assessment (with system owner and stakeholder input).

Gaps are identified and developed into Risks, Issues and Opportunities for prioritization by leadership.

Identify Risks, Issues and Opportunities.

Describe target security posture.

Determine target security posture, based on:
- Business needs,
- Current staffing
- Current/projected budget
- Timeframe
- Mission/operational priorities
- Threat environment
- Impact