Chinook
Secure · Compliant · Efficient

Capabilities Statement

Security & Resilience

Your buildings deserve the best you can give them. Your mission, your occupants, and your budget depend on it.

Chinook has leveraged our extensive history of facility engineering and building commissioning, as well as our subject matter expertise of building control systems, to create a comprehensive System Security Engineering (SSE) program following industry standards for facility-related control systems (IEC, ISA, NIST, IEEE, UFC 04-010-06). Our SSE team combines the skillsets of cybersecurity and facility controls specialists focused on implementing defense-in-depth strategies to optimize intelligent building systems and mitigate risks and attacks. Our SEE program takes a hands-on and detailed approach to identify and mitigate system security vulnerabilities during design, development, implementation, and acceptance testing to ensure delivery of secure end-to-end systems.

- **Design/Build**: Chinook's role on this project is to ensure the FRCSs are planned, designed, acquired and executed in accordance with UFC 4-010-06 "Cybersecurity of Facility-Related Control Systems," and as required by individual Service Implementation Policies. Chinook's approach to managing the cybersecurity process is to facilitate an integrated team effort involving representation from stakeholders committed to the project delivery and occupant program requirements.
- **Physical & Logical Inventory**: Chinook has provided Facility Related Control System (FRCS) Inventories and providing Risk Management Framework (RMF) recommendations with cost estimates for 3,500 buildings, totaling approximately 40 million square feet (SF) and spread across 52 CONUS and OCONUS locations. Work consists of onsite surveys, threat/hazard analysis, network discovery, network traffic analysis, vulnerability analysis and reporting.
- **Procure & Install**: Chinook has designed, procured and installed IT equipment for control systems to include: virtualization host servers, physical domain controllers, time synchronization servers, network switches, rack monitors and KVM switches, operator workstations and monitors, and maintenance laptops.
- **Portfolio-Based Risk Assessments**: Implementation of a cybersecurity program for Facility Related Control Systems (FRCS) consisting of a multi-tiered risk assessment methodology per National Institute of Standards and Technology (NIST) SP-800-37. Chinook works with stakeholders to conduct risk assessments across a representative sample of buildings within their portfolio. We establish client-specific metrics to capture impacts to organization, various mission/business functions and systems, and interconnections. Our team utilizes a network discovery appliance to capture asset inventory and identify vulnerabilities at each location. Threat sources are paired to each vulnerability to calculate the overall likelihood of impact ultimately quantifying a risk score for the organization.

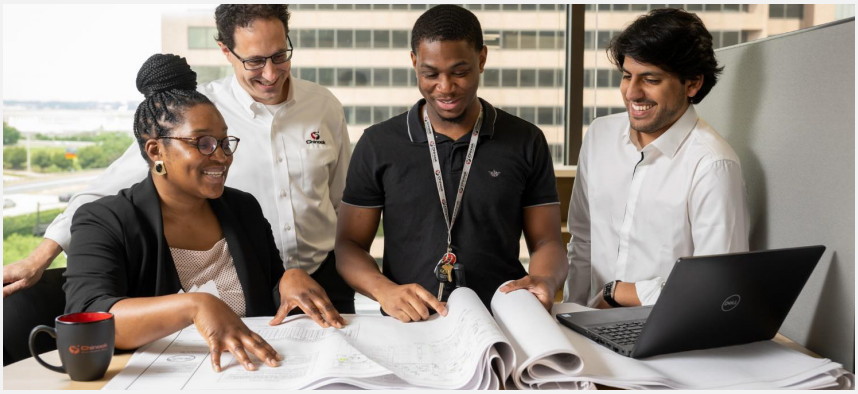
Infrastructure Sectors

- Government
- Healthcare
- Defense Industrial
- Education
- Commercial
- Telecommunications

Chinook
Secure · Compliant · Efficient

Capabilities Statement

Security & Resilience



Our SSE team is comprised of employees and partners who are the leading cyber experts in OT and IT. Our experts include:

5 Security+ Professionals

2 Certified Information Systems Security Professionals (CISSP)

1 Global Industrial Cyber Security Professional (GICSP)

1 Certified Ethical Hacker (CEH) Professional

Technology

Network Discovery
Vulnerability Analysis
Compliance Verification
Cybersecurity Laboratory
Asset Management

Services

OT/FRCS Cybersecurity
Portfolio-Based Risk Assessments
Risk Management Framework
Design Phase Services
UFGS 25 05 11 & UFGS 25 08 11
Cybersecurity Subject Matter Expertise
Continuous Monitoring & Change
Control Board (CCB) Support
Physical & Logical Inventory

Equipment

Field Survey Tool Kits
Nozomi Guardian Appliances

Featured Projects

U.S. Army Reserve / Facility-Related Controls Systems Inventory and Risk Management Framework / *Nationwide Locations*

Missile Defense Agency / Facility-Related Controls Systems Inventory and Risk Management Framework / *Nationwide Locations*

Missile Defense Agency / Building Automation System Cybersecurity / *Fort Greely, AK*

National Geospatial-Intelligence Agency / Cybersecurity / *Springfield, VA & St. Louis, MO*

Fort Shafter Command & Control Facility / Phase 3 Cybersecurity / *Fort Shafter, HI*

U.S. Army Intelligence & Security Command (INSCOM) / Nicholson Building Risk Management Framework (RMF) / *Rivanna Station, VA*

Naval Surface Warfare Center, Crane Division / Cybersecurity / *Crane, IN*

Contacts

Matthew Steeves, CISSP, CEH, CPT, CxA, DGCP
Program Manager, Security & Resiliency
O: 703.216.5652
E: msteeves@chinooksystems.com

Tom Froass CISSP, Security+ CE
Cybersecurity Project Manager
E: tfroass@chinooksystems.com