KARTHIK CONSULTING
Beyond the expected

3120 Fairview Park Drive
Suite 800
Falls Church, VA 22042
www.karthikconsulting.com

AT A GLANCE

NAVFAC – Cyber Security + Network Facilities Management

KEY STATS

CYBER AND PROGRAM MANAGEMENT

- Provided Risk Management Framework (RMF) expertise supporting the issuance of two three-year Authority to Operate (ATO)
- Reviewed 3,500 security controls, developed 5,200 plan of action & project milestones, and developed ISSE Handbook
- Participated in Europe based RMF 3-step assessment of power generator system
- Developed policy development capability utilizing SharePoint Online reducing time to develop policies by 75%
- Completed detailed site surveys identifying FRCS and supporting infrastructure for Far East based installations
- Supported stand-up of Cyber Planning and Response Center (CPRC) team with Threat Hunting, Penetration Testing, and Malware analysis
- Executed cyber top table exercise and response plans, including SOP's
- Supported CYBERSAFE grading and critical analysis trainings
- Managed CCB framework and accountability planning

SIZE AND SCALE OF KC SUPPORTED SYSTEMS

- 4 Echelon III CIO orgs
- 9 Facility Engineering Commands (FECs)
- 35 FRCS across the globe
- 150 RMF milestone events

KC CUSTOMER IN FOCUS.

The Naval Facilities Engineering Systems Command (NAVFAC) bears the significant responsibility of delivering facilities engineering solutions for the entire U.S. Navy and Marine Corp. NAVFAC has more than 17,000 employees across the globe. As the facilities manager for the Navy, NAVFAC is responsible for Facilities Related Control Systems (FRCS), including supervisory control and data acquisition (SCADA) systems – which are often used in industrial operations to monitor and control field devices – as well as its cybersecurity policies. NAVFAC is also the Department of the Navy's Technical Authority and overall lead agency for Cyber Security for Facilities/Industrial Control Systems (ICSs).

SIGNIFICANCE OF REQUIREMENTS.

In the U.S. Navy, SCADA systems can be found in ashore facilities ranging from Command Centers to warehouses that store chemicals and ammunition. Given the critical nature of the Navy's mission, the security of these technologies – regardless of their location across the globe – is essential.

Continued on next page

NAVFAC is responsible for ensuring that the Navy's cyber networks employ the most rigorous cybersecurity standards, such as those recommended through the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), and applying them to ICS everywhere from Guam to Europe to Africa to NATO locations. NAVFAC must identify vulnerabilities in the cybersecurity process that could weaken the Navy's security.

OPPORTUNITY FOR KC IMPACT.
The organization required an enterprise-level process and methodology for authorization when new FRCSs came online. In addition, the Information Systems Security Manager (ISSM) and Information Systems Security Officer (ISSO) needed assistance in mission critical support regarding risk management and analysis. NAVFAC also required support of numerous cyber systems, including ICS, FRCS, and operational technology.

DELIVERED RESULTS.
KC provided risk analysis and systems/cyber engineering support to NAVFAC Information Technology and Operational Technology (IT/OT) systems to help bolster and protect the Navy's global infrastructure against threats. KC also supported the Command Information Office (CIO) and the Command Information Security Officer (CISO)/Director of Cybersecurity through project management, planning, analysis, and more.

KEY AREAS OF KC IMPACT.

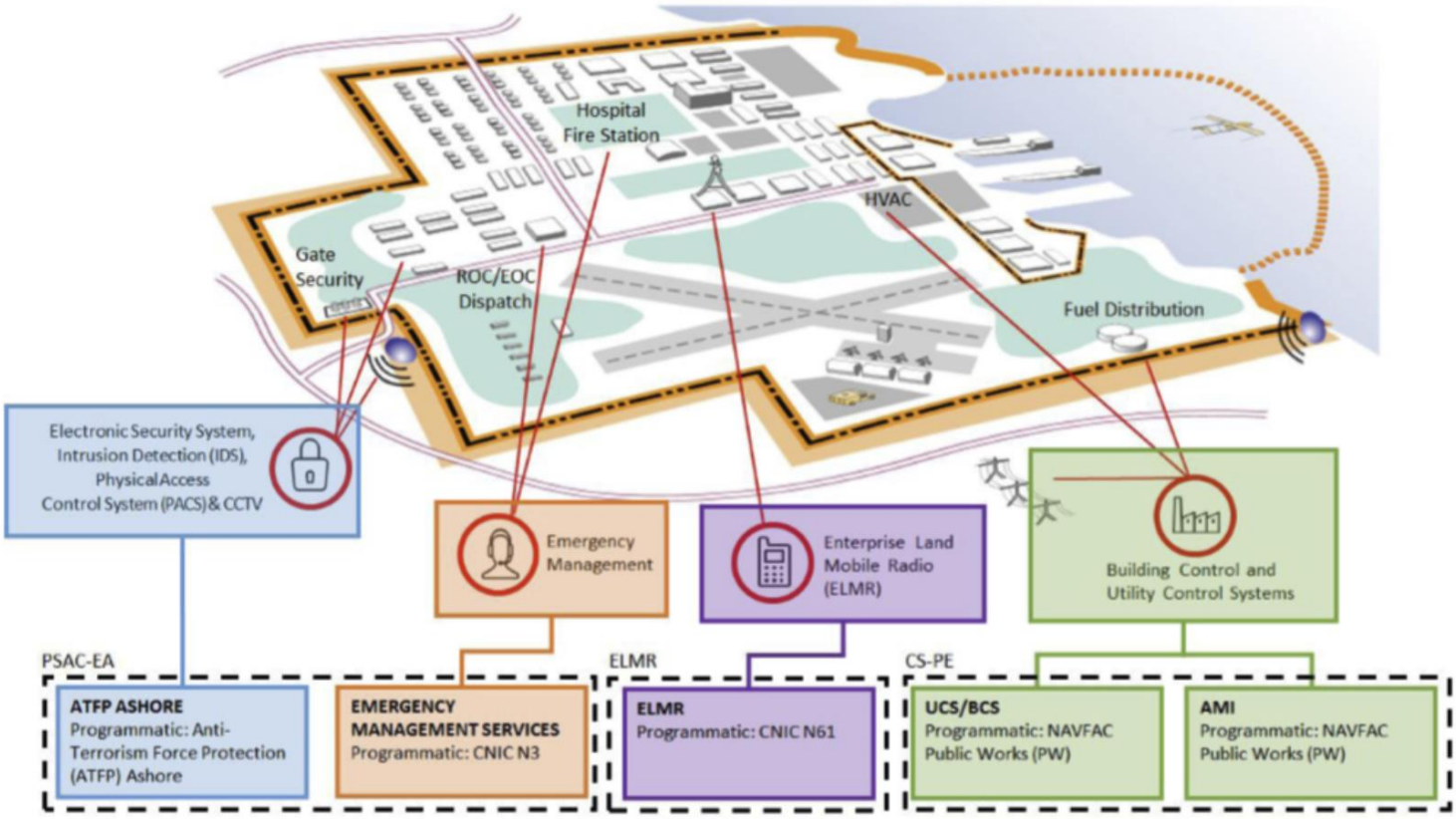
COMMAND INFORMATION OFFICE (CIO) SUPPORT:

- Project management, scheduling, KPI/cybersecurity metrics.
- Develop project plans and briefings to support various Cybersecurity initiatives and stakeholder forums.
- Maintain quality assurance.
- Training activities and technology analysis.
- Alignment of IT solutions with the command's data management policies and enterprise architecture strategy.
- Technical reporting and documentation.
- Enterprise Change Control Board (ECCB) management.
- RMF packages: including Memorandums for the Record (MFRs)
- Response to Cyber Technical Advisories (CTAs) and Information Assurance Vulnerability Management (IAVM) directives.
- Employ systems concepts and capabilities phases for development life cycle.
- Ensure security design and implementation of systems/programs in accordance with governing NIST, DoD and DON requirements/standards.
- Manage checkpoint/collaboration meetings to review RMF status for NAVFAC FRCS.

"Karthik's cyber expertise has been critical to some of NAVFACs most critical programs including Cybersecurity, Risk Management Framework (RMF) Steps 1-3+, and CYBERSAFE criticality analysis."

– Reported in CPARS from NAVFAC HQ CIO Team

Continued on next page



Source: NAVFAC Cybersecurity Way Forward, 10 December 2019

RISK ANALYSIS TECHNICAL SUPPORT:

- Led collaboration process to help identify, access, analyze, and manage cyber risk to protect NAVFAC data. Managed assessment, maintenance and restoration of information systems incorporating protection, detection, and reaction capabilities.
- Maintained federal cybersecurity instructions, policies, procedures, directives, methodologies, and security orders.
- Oversaw reporting of cybersecurity events and incidents.
- Conducted compliance audits, developed cybersecurity awareness products and training, and continuously assessed the effectiveness of policies security SOP's.

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

- Develop, maintain, and update RMF technical artifacts.
- Support the government Information System Security Manager (ISSM).
- Provides support to help implement cybersecurity for the respective NAVFAC programs, organizations, systems, or enclaves.

INFORMATION SYSTEMS SECURITY ENGINEERING (ISSE)

- Played integral role on the IT/OT systems engineering and security response teams to ensure that cybersecurity solutions are effective and efficient.
- Provide full security engineering and review services.
- Develops and maintains the cybersecurity architecture of a program.

Continued on next page

CYBER PLANNING AND RESPONSE CENTER SUPPORT

- Provided consultation on Red Team capabilities, organizational structure, CPRC Red Team documentation
- Provide reference resources for Key Management Infrastructure cryptologic devices
- Provide introductory touchpoints back to the National Security Agency for collaboration

MANAGEMENT NETWORK ENGINEERING

- Design system configuration, directing system installation, and define, documenting, and enforce system standards.
- Maximize network performance by monitoring performance, troubleshoot network problems and outages, schedule upgrades.
- Maintain security of network systems through enforcing policies and access protocols.

CONTROL SYSTEMS ADMINISTRATION

- Manage the process of systems configuration, maintenance, and cyber security compliance.
- Employ best practices and expertise to effectively manage FRCS configuration.

CRITICALITY ANALYSIS SUPPORT

- Ensure Cybersecurity Safety (CYBERSAFE) grading activities are executed and tracked per defined parameters.
- Manage the analysis, coordination, integration, and implementation of policies and procedure updates.
- Support the decomposition of systems supporting priority assets in accordance with NAVFAC/DON/DoD directives.

SYSTEMS ENGINEERING TECHNICAL REVIEW (SETR)

- Provides SETR support to NAVFAC: includes building, deploying, and managing the NAVFAC enterprise SETR process(es).
- Provides expertise across multiple systems engineering disciplines to ensure the SETR meets DON standards, is tailored to address Command-specific efforts, and meets integration/interoperability concepts supporting IT/OT interfaces.

ABOUT US

Karthik Consulting was founded in 2008 to be a reliable and trusted advisor for our customers, providing independent, unbiased, and proven solutions that mitigate risk and help solve enterprise-wide IT challenges.

Our Cyber Security, Software Development and Program Management focus areas (and work methodology) ensure that we can deliver not just solutions, but architecture that scales and grows with the customer's needs over time. We are able to assist in projects ranging from short advisory engagements to assembling a full team to deliver a solution from concept through implementation and on-going management. KC has access to industry experts in various technologies and teaming partners to meet any of your IT challenges. The vision of KC is to bring the innovation, passion and agility of the commercial IT industry to meet the unique challenges of the federal government. We are a DOD Cleared Facility with a DCAA-approved accounting system.

CAGE: 56GH3
DUNS: 828199880
UEI: FGNNM7KNUPF6

CONTACT

Felix Martin, 571-765-2567
fmartin@karthikconsulting.com

PRIME CONTRACT VEHICLES

GSA MAS (IT-70)
GSA OASIS Pool 1 and 3
NIH CIO-SP3 8(a) and SB
Army RS3
Navy Seaport-NexGen
FAA eFAST
GSA 8(a) STARS III (via JV)
Air Force SBEAS (via JV)