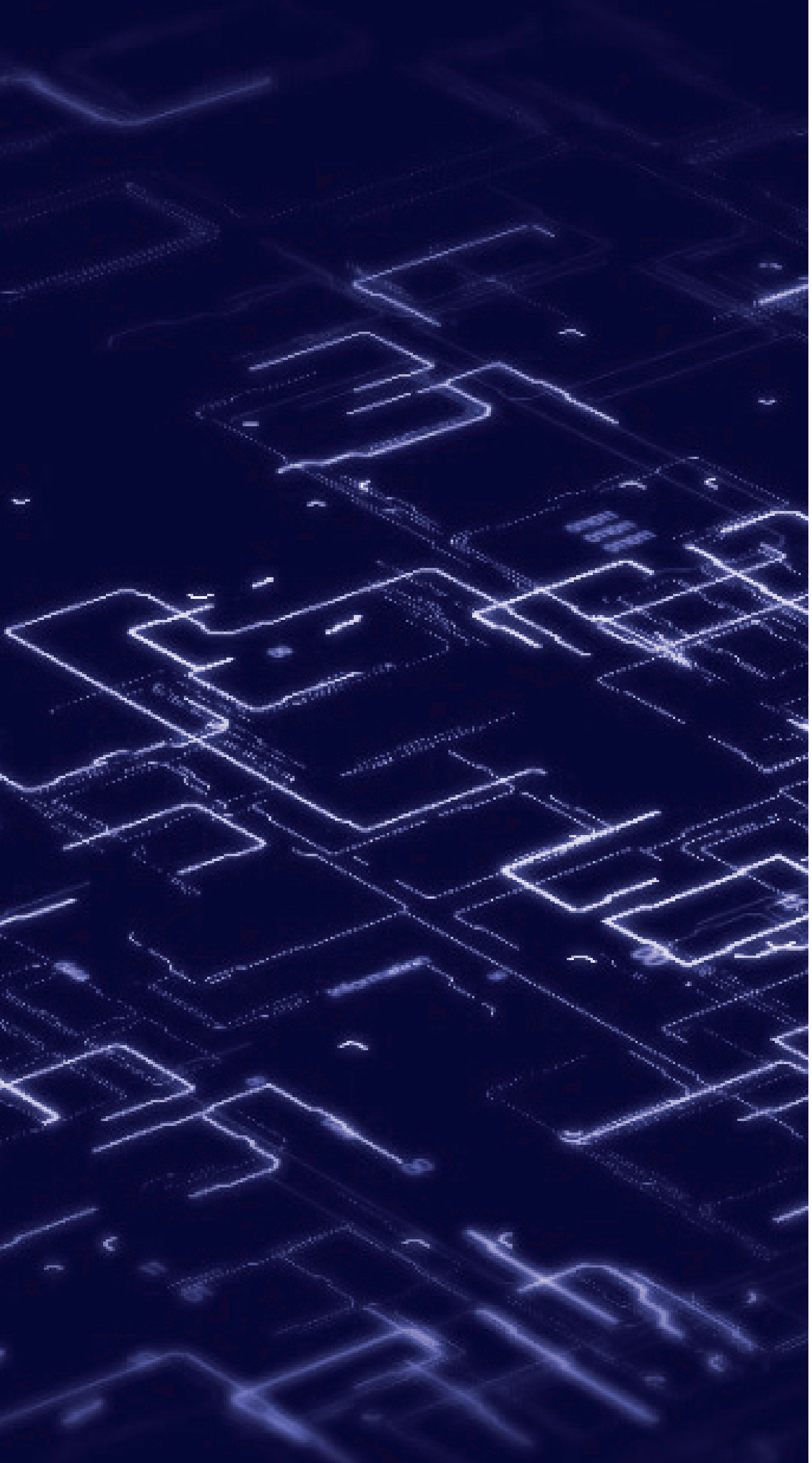
ELLIOTT MANAGEMENT LLC

Service Catalog



About Us

Elliott Management LLC (EM) was established by a Disabled Veterans with over 20 years of total experience in the security profession. EM was formed in 2018 and is dedicated to providing exceptional security services.

Our Mission is to provide incomparable services and acute resolutions to meet our customers' needs while controlling costs. EM places innovation and security at the core of all our business services.

EM is a nationally operating Service-connected Disabled Veteran Owned Small Business (SDVOSB) that provides a wide range of consulting, operations, program management, and technology services to federal, state, and local government entities and to private institutions across the nation.

Our team supports your information systems and networks with cradle-to-grave hands-on solutions.

A Solid Reputation

Reputation is everything regarding security, and a good reputation is built on brilliance, reliability, and assurance – and that is precisely what we provide.

What Makes Us Different

Our team consists of federally trained cybersecurity professionals who have secured some of the nation's most critical capabilities, information systems, and technologies. We have assessed, controlled, and continuously monitored systems under direct attack from adversaries. Our approach is to bring you the same level of professionalism and protection.

Service-connected Disabled Veteran Owned Small Business who hires Veterans. What you get when you hire this veteran-owned business is the same commitment to the mission. As a veteran, the mission comes first. You and your cybersecurity are our mission, and nothing will come in between us and completing our mission!

Why is Cybersecurity Important?

Cybersecurity is more critical than ever in a world where every day, more business and financial decisions are made online. Families, governments, and companies must protect themselves from unseen cyber threats.

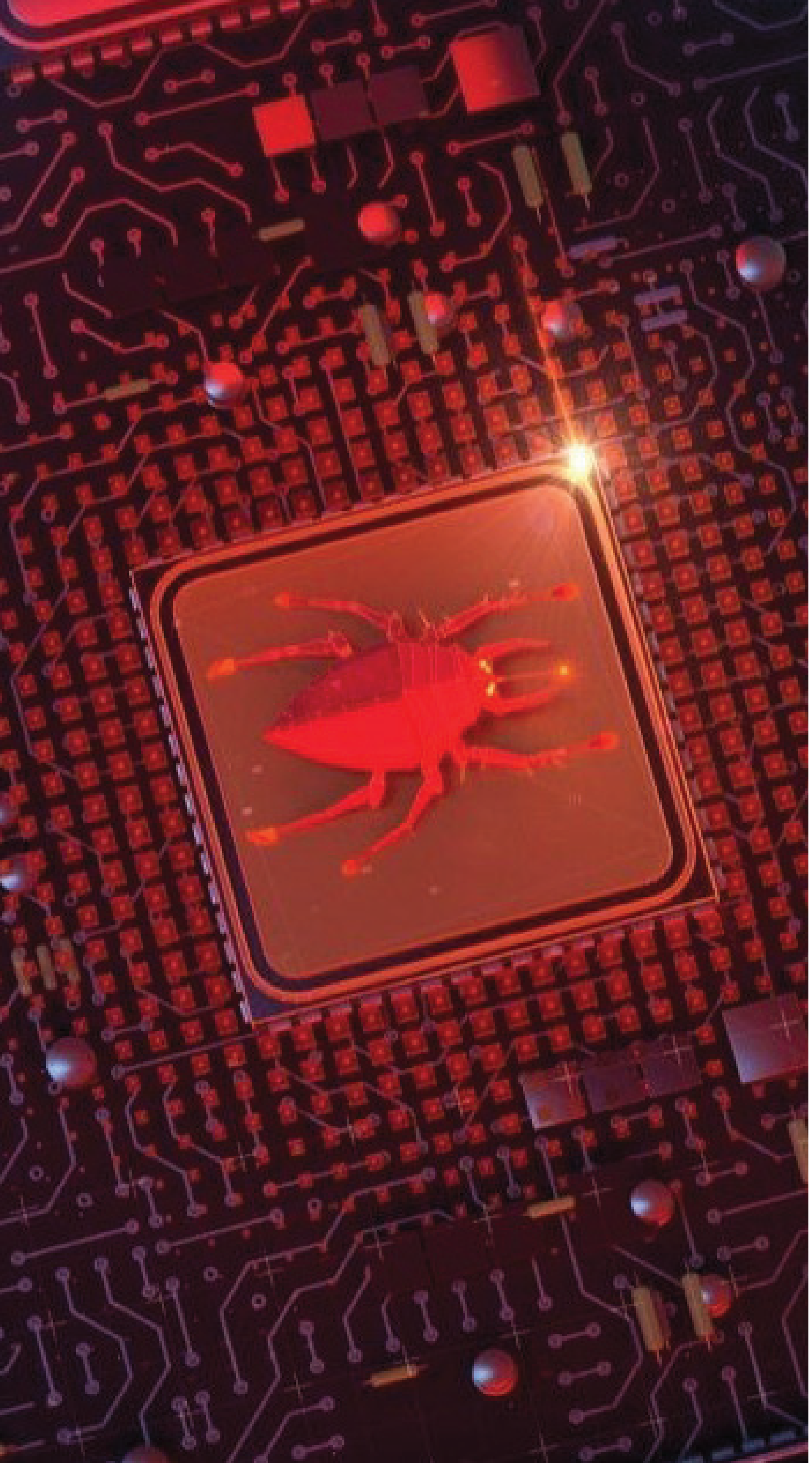
Protecting Information, Information Systems & Networks

We take the time to understand what needs to be protected and why. From there, we focus on developing the best how and evolving it as risk evolves. Our approach is to listen

- We have dedicated Project Managers who delicately manage everything from onboarding to offboarding.
- We are hands-on with the solutions we implement. We also take the time to educate the business on the risks, mitigations, and our continuous monitoring process. We want the business to be active partners in their cybersecurity.

How We Help Our Clients

- We can assess your risk.
- Help identify your acceptable level of risk.
- Develop a risk mitigation strategy based on your acceptable risk level.
- Develop a customized solution and strategy.
- Implement customized solutions.
- Continuously monitor for new and evolving risks.



Cybersecurity

Elliot Management's (EM) approach is rooted in the principal requirements of secure networks and information systems. Our team leads from the front, providing unrivaled services and solutions and ensuring your organization's deliverables are uncompromising. Risk management plans are designed, implemented, and continuously monitored to ensure we are providing our customers with an unmatched assurance level.

There is a lot to consider when seeking agile and reliable security solutions—our full range of reliable and decisive solution-based services can meet the needs of your organization.

Our Experience

Working with our clients to overcome challenges and provide actionable solutions

EM's client had challenges making informed cybersecurity decisions on software procurement without painstaking delays. Our team interviewed the various stakeholders, both internal and external, who were involved in the decision-making process. We identified the roadblock, redesigned the department's decision-making process, and aligned it with an effective process. We eradicated their delayed approval process, decisions were made promptly, and the promotion of cybersecurity became priority number one.

Our Clients Include

- Air Force Global Strike Command
- American Rheinmetall Vehicles
- Apollo Information Systems, Corp
- Defense Counterintelligence Security Agency (DCSA)
- Defense Intelligence Agency (DIA)
- Matrix Metals
- National Geospatial-intelligence Agency (NGA)
- Office of Special Investigation-Special Project and Special Power Sources.

Cybersecurity Offerings

Cybersecurity Assessments

Conduct a rigorous test and evaluation of organizational cyber assets, individuals, security profiles, and readiness of automated, physical, and technical controls, policies, procedures, and governance. We determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements of the system(s). Our meticulous security control assessors are detailed, organized, thorough, and highly experienced in evaluating your Information Systems security posture.

Cybersecurity Assurance

Provide complete lifecycle management support to information systems and networks governed by Air Force Instructions, Cybersecurity Maturity Model Certification, the Defense Assessment & Authorization Program Manual, Federal Information Systems Modernization Act, Health Insurance Portability and Accountability Act, Joint Special Access Program Implementation Guide, National Industrial of Standards and Technology, Payment Card Industry, and other standards.

Our Subject Matter Experts possess an array of industry-recognized cybersecurity certifications.

Cybersecurity Engineering

Identify critical assets (e.g., networks, topology) and external dependencies; develop measures and policies commensurate to the risk profile. We capture and refine information security requirements and ensure the integration of information technology component products and information systems through purposeful security design or configuration.

Cybersecurity Governance

Define your risk management policies, strategy, and goals. We work with senior leadership to design road maps to maintain and improve your overall risk management approach. We develop, modify, and update standardized processes and assist with accountability and consistency of documented governance.

Cybersecurity Lifecycle Support

Identify your critical assets (e.g., networks, protocols, and topology) and external dependencies. Our team then develops measures and policies commensurate to the documented risk profile and implements them. We establish, modify, and continuously monitor business continuity procedures; leverage lessons learned to ensure applied solutions mitigate up-to-date risks. We ensure a plan of action and milestones (POA&M) is maintained, reviewed, and modified quarterly in conjunction with a quarterly system or network health report.

Cybersecurity Maturity Model Certification (CMMC) Support

Provide consultation and pre-assessment services of customers' CMMC posture and provide recommendations.

We have Registered Practitioners on our team and are awaiting our Certified Third-Party Assessor (C3PAO) certification.

Vulnerability Assessments

Perform Tenable and Security Content Automation Protocol examination of information systems pinpointing security deficiencies in the operating system, applications, and configuration. We provide solutions to the vulnerabilities and confirm the adequacy of such measures after implementation.

Cybersecurity Services

Health Check Security Review

Identify the strengths and weaknesses in an organization's security controls. We will evaluate hardware and software systems, networks, clouds, databases, and third parties.

Security Assessment & Roadmap

Assess your security program, including people, operating models, and tools. We will deliver a complete understanding of your security risk in business terms which will initiate the building of a long-term security program. The roadmap for elevating your organization's security program will balance the business needs, the risks, and the organization's acceptable investment.

Threat Assessment

Identify and assess the risks to which an organization and its assets are exposed to cyber hacker groups. Our Analysts will identify likely threats from known and unknown threats relevant to your specific business. They will identify attack surfaces using open-source and proprietary security intelligence sources.

Penetration Testing

External Penetration Testing — Perform penetration tests on the internet points of presence, including internet protocols (IP) and domains for externally facing websites, both on-premises and cloud-based.

Internal Penetration Testing — Perform penetration tests on internal data networks with or without IT team knowledge. These tests are designed to identify significant known network vulnerabilities and categorize and prioritize them for remediation.

Social Engineering — Target and take advantage of the human element to gain access to your network. During an assessment, various methods will be used to gain information that may assist in future attacks, gather valid user credentials, or gain a foothold on the internal network.

EM's test methodology is based on industry best practices and includes the following:

- Open Web Application Security Project (OWASP) Testing Guide
- NIST SP 800-15, Technical Guide for Information Security Testing and Assessment
- The Penetration Testing Execution Standards (PTES)
- Payment Card Industry (PCI) Penetration Testing Guidance

Security Engineering

The core of security operation programs is the ability to assess and define secure practices and their implementations. Whether it's the design of network or application controls, cloud security architecture, mobile devices, online social media, or critical 3rd parties, all requirements must be correctly engineered and integrated into the security program.

EM provides security engineers to design and implement all the products and services we office, including:

Security Design Review — Review of the security controls in place and their effectiveness against the threats the organization or systems faces.

Security Risk Assessment — A combination of security design review and defined penetration testing services to validate risk from the hacker's perspective.

Security Engineering Review — A review of the developed design by our Security Engineers to evaluate the architectural model in use and the gaps in need of repair and upgrade to protect the organization or product.

Data Privacy

Provide professional assessment and development services for all major privacy regulatory requirements. We develop optimized governance structures and systems, including data identification and mapping, data and metrics definition, process integration, and program oversight integration.

Disaster Recovery

The Disaster Recovery Program for organizations starts with a fundamental understanding of the current technology and the development of the required playbooks for recovery scenarios. Our program includes the best practice steps or can be configured to focus on specific pieces of an existing program to improve maturity.

Education & Training

Perform tailor-made cybersecurity awareness training for organizations. We develop technical and specialized training from the executive teams and the incident commander to the systems administrators and general users.

Incident Response

Incident Response - Planning & Management — Build Incident Response (IR) programs that can integrate into overall business plans. IR plans become critical and streamline the coordination as an incident escalates and begins to impact company-wide or the public.

Tabletop Exercise & Testing — Use industry-recognized best practices to quickly explore and improve incident response plans in our tabletop exercises.

Risk Assessments

Identify and prioritize vulnerabilities to help organizations prevent, detect, and respond to cyber-attacks. We also perform comprehensive risk assessments to identify potential technologies, procedures, and controls to mitigate the identified risks.

Security Scanning

Use solutions to scan internal and external networks for vulnerabilities, misconfigurations, and unintended connection activity.

Governance, Risk & Compliance Services

Security Governance

Develop robust security governance which delivers key capabilities:

- Enable the timely review of risk data and effective decision-making
- Create defined and implementable roles, responsibilities, processes, and procedures to facilitate processes
- Enable technology to support the collection, processing, and reporting of relevant risk data for governance review
- Ensure personnel are trained appropriately to collect and interpret the correct information, adjust collection based on changes in the risk profile and communicate to all levels of the organizations

Cybersecurity Frameworks

Cybersecurity Frameworks are a necessary part of security compliance programs. We build compliance framework programs to meet:

- Center for Internet Security Standards (CIS Top 20)
- National Institute of Standards & Technology Cybersecurity Framework (NIST CSF)
- National Institute of Standards & Technology Special Publication 800-53
- National Institute of Standards & Technology Special Publication 800-171
- Open Web Application Security Project Top 10 (OWASP)

Security Risk Management

EM's risk management program incorporates commercially reasonable regulatory compliance, benchmarking against industry frameworks and maturity models, and robust business-driven holistic risk management.

Our program includes:

- Risk Assessment
- Risk Register
- Vendor & 3rd Party Security
- IT Project Risk Assessment
- Situational Awareness Testing
- Security Awareness & Training

Cybersecurity Compliance

Compliance Frameworks have defined testing and audit requirements for an organization's compliance. These frameworks are defined by government or oversight bodies and require organizations to comply with the specified requirements. Often, independent third parties are used as inspectors to evaluate and confirm compliance levels.

Our team builds compliance programs for:

- **Gramm-Leach-Bliley Act (GLBA)** — Financial Services regulation that includes cybersecurity requirements
- **Cybersecurity Maturity Model Certification (CMMC)** — Requirement for cybersecurity standards to serve DoD contracts
- **Sarbanes Oxley Act (SOX)** — Information requirement for Publicly traded companies
- **Federal Risk and Authorization Management Program (FedRAMP)** — US Government requirements for cloud security
- **North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)** — Standards used to secure the bulk electrical system
- **Payment Card Industry Data Security Standard (PCI DSS)** — the industry standard for credit card companies and vendors

Compliance with the Federal Cyber Guidance

- Air Force Instructions (AFIs)
- Army Regulations (AR)
- Committee of National Security Systems (CNSS)
- Cybersecurity Maturity Model Certification (CMMC)
- Defense Counterintelligence Security Agency (DCSA) Assessment and Authorization Policy Manual (DAAPM)
- Department of Defense Directive 8570.01 and 8140
- Department of Defense Instruction 8510.01
- National Institute of Standards and Technology (NIST)

National Industrial Security Program (NISP) Compliance

Assist with the Defense Counterintelligence and Security Agency (DCSA) – Security Vulnerability Assessments preparation and resolution of findings. We offer Independent NISP assessments, customized NISP training and compliance, and Facility Security Officer (FSO) support.

Insider Threat Program Development

Develop insider threat programs per National Industrial Security Program (NISP) requirements. We also provide technology and process tools to assess and measure insider risk and abnormal user behavior.

Enterprise IT

Everyone seeks ways to develop and maintain a contemporary, agile, effective, and secure IT infrastructure. IT transformation doesn't necessarily mean wholesale change. Transforming your IT can be as minimal as improving legacy systems to support simple-to-use operating systems or augmenting platforms that deliver an efficient and user-friendly experience.

The Importance of Enterprise IT

Core organizational business activities take place on your enterprise IT. Having the proper hardware and software solutions helps streamline business functions and productivity. Whether on-premise or in the cloud, the management of these core organizational services goes beyond just taking care of the technology.

What's Our Differentiating Factor?

What makes us different is that we will never push more technology or software unless necessary for your business functions. We focus on your current technology to determine if it is being used to its fullest potential. We also ensure your technology solution will be designed with security in mind.

Our Experience

Working with our clients to overcome challenges and provide actionable solutions

We've helped clients with the scope development, planning, and execution of technology refresh. The technology refresh consisted of millions of dollars of hardware and software at several locations in the United States, Europe, and Asia-Pacific.

Enterprise IT Services

CISO Services

Offer on-call, temporary, and interim subject-matter advice for organizations facing complex business decisions where cybersecurity is a risk. The ability to have one of our professionals providing strategic advisement, supporting 1-on-1 discussion on security topics and management support, will be a luxury our competitors cannot match.

Cloud Security

Establish policies, technologies, applications, and controls to protect the virtualized internet protocols, data, applications, and services associated with your environment. We focus on deterrent, preventative, detectives, and corrective controls to give you the required to operate cost-effectively and securely.

Data Protection & Privacy

Assess and identify risks to data privacy by gauging systems, programs, products, or service impacts following local, state, and federal laws for data processing.

IT Program Consulting

Advise on services that can help clients assess different technology, business, and process strategies.

IT Asset Management

Join financial contractual and inventory functions to support the lifecycle management and strategic decision-making for your IT environment. Our solutions deliver:

- Greater flexibility in IT service delivery,
- Increased cost savings from effective IT inventory management,
- Improved service outcomes by aligning IT spending, and
- Reduction of risk and vulnerabilities by keeping end-of-life hardware and software off the enterprise network can benefit from our result-driven IT Asset Management team.

IT Project Management

Oversee the IT execution and management by incorporating government and commercial best practices through dependable, repeatable processes that provide standard configuration for planning and management oversight through the project lifecycle.

IT Strategy Development

Assist organizations in cultivating IT strategies for delivering services and managing their IT portfolio. Our team develops a tailored phased approach with each phase containing executable and logical groupings.

Managed Security Services

Manage all your cyber and IT security-related needs consisting of Implementation and Staging, Network Consulting, Audits, Cybersecurity and Patch Management, Configuration Management, and Backup and Recovery on a proactive basis.

Security Advisory & Operations Services

Provide our clients with the vision and mitigation strategy to defend against cyber adversaries and reduce their exposure to threats targeting applications, hardware, and other enterprise assets.

System Administration

Supports the installation and maintenance of information systems and networks and ensures effective information system utilization, adequate security parameters, and proper implementation of established computer security policies and procedures.

Security Management

A superior security management program begins with a basic understanding National Industrial Security Program Operating Manual (NISPOM). Our experts have perfected the art of Security Management in various disciplines, including Collateral, Operations Security (OPSEC), Sensitive Compartmented Information (SCI), and Special Programs.

The Importance of Security Management

Things can sometimes be overlooked inadvertently for organizations new to the Defense Industrial Base. The same applies to a much more seasoned organization performing security management. A mistake can result in the loss of a security clearance, a security infraction, or a security violation. No one wants their business or personal livelihood jeopardized due to security violations.

How We Are Different

Our in-depth experience and knowledge of the NISPOM, the DoD Manuals, the Intelligence Community Directives, the Air Force Instructions, the Naval Administrative Messages (NAVADMIN), and the Army Regulations (AR) are unmatched. That level of expertise allows us to interpret and implement the guidance to meet the needs of your security program. We also have the relationships within these services and governing bodies to get the answers you need to ensure you meet the regulations' intent and letter.

Our Experience

Working with our clients to overcome challenges and provide actionable solutions

A customer needed to establish a clear information system to perform the duties identified in their statement of work as a new Defense Industrial Base (DIB) contractor.

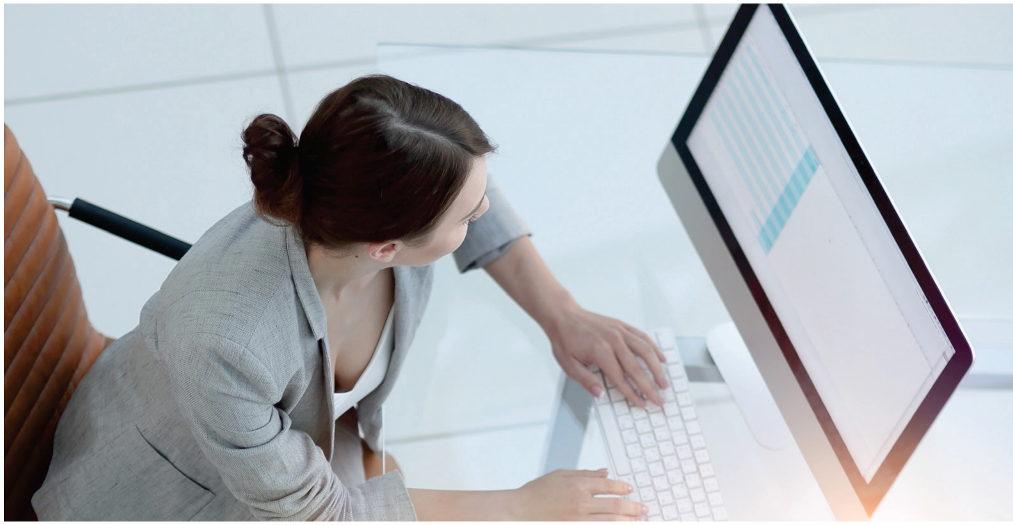
EM developed the security program and the Authority to Operate (ATO) packages for the organization as they were new to the DIB and did not have a qualified Facility Security Officer or an Information System Security Manager with the proper level of understanding of the Defense Counterintelligence Security Agency Assessment and Authorization Manual (DAAPM) and National Industrial Security Operating Manual (NISPOM).

Our High-Impact Solutions

A client that had been in their facility for over 40 years had to be out of the leased facility within 30 days. Maintaining productivity was imperative to this organization and its mission. We helped the client identify a plan to relocate their information systems to two separate facilities they had in the deep south and Midwest. Our team devised a solution to ensure processing could continue and the destruction of materials no longer needed. Our team worked with our client to implement the plan and get it approved by the Program Security Officer. We coordinated the plan, executed destruction runs, and executed the move flawlessly, all within 22 days.

Our Clients Include

- American Rheinmetall Vehicles
- Ball Aerospace
- General Dynamics Information Technology
- L3Harris Technologies
- ManTech International
- Matrix Metals
- Office of Special Investigations – Special Project (OSI-P)
- Raytheon Technologies



Operations Security (OPSEC) Program Assessments

Employ a five-step OPSEC process to deliver strategic, tactical, and operational assessments on physical, personnel, access controls, and other critical OPSEC systems assessments. We are experts in evaluating commercial, residential, educational, mixed-use, or industrial facility footprints for operations security.

Security Management

Perform cradle-to-grave security support for sensitive and special programs. We help interpret and implement tailored security solutions. Whether its Establishment, Management and Administration, Apportionment, and Disestablishment of programs, we can support all your needs.

The EM team are experts in the Department of Defense Manual (DoDM) 5200.01 Volume 1 – 3, DoDM 5205.07 Volume 1 – 4, Intelligence Community Directives (ICD) 703, 704, 705, and 710, and NISPOM. Our services include:

Our services include:

- Classification Management
- Document Control
- Industrial Security
- Information Security
- Operations Security
- Personnel Security
- Physical Security
- Program Security

Special Access Programs (SAP) / Sensitive Compartmented Information (SCI) Program Security Support

Cradle-to-grave security support for collateral, compartmented and special programs in compliance with DoDMs, Intelligence Community Directives (ICDs), and NISPOM.

Help interpret and implement tailored security solutions for programs throughout the Establishment, Apportionment, Management/Administration, and Disestablishment phases.

Our services include:

- Classification Management
- Document Control
- Industrial Security
- Information Security
- Operations Security (OPSEC)
- Personnel Security (PERSEC)
- Physical Security

Secure Destruction Run Coordination & Execution

Plan, coordinate, and execute the destruction of SAP and SCI information technology equipment. We have coordinated over ten (10) destruction runs flawlessly and to the satisfaction of the Office of Special Investigation-Special Projects (OSI-PJ) Program Security Officer.

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Cybercrime Magazine (2020)

Cybercrime cost U.S. businesses more than $6.9 billion in 2021, and only 43% of businesses feel financially prepared to face a cyberattack in 2022 – Forbes (Nov 2022)

Elliott Management LLC. specializes in predicting, mitigating, and shutting down cyber threats so you can be on the offense rather than defense. **We're here to help you!**

ELLIOTT
MANAGEMENT
LLC

610 Uptown Boulevard, Suite 2000
Cedar Hill, TX 75104
Telephone: 469.523.1358

109 E. 17th Street, Suite 5800
Cheyenne, WY 82001

720 S. Colorado Blvd.,
Penthouse North,
Denver, Colorado, 80246

Email: elliott@ellimgmt.com

ELLIMGMT.COM