NGA
Cybersecurity Strategy 2023

Securing the GEOINT Advantage

Approved for public release, NGA-U-2023-02442

Foreword & Introduction

Letter from the Director

Team NGA,

Cybersecurity is a lifeline for NGA's business and mission operations. Our nation relies on us to sustain GEOINT (Geospatial Intelligence) advantage and to be ready to respond to future challenges. Without a secure information technology ecosystem, the Agency's ability to source, store, and disseminate GEOINT for our nation's warfighters, policymakers, and intelligence professionals is jeopardized. Our adversaries know this and constantly try to penetrate our networks, attempting to degrade our capabilities and erode trust in the reliability of our products and services.

From performing basic cyber hygiene to deploying sophisticated deterrence to supply chain risk management, our focus is on thwarting adversaries' efforts to deny us capability. As part of this collective enterprise-wide effort, we have an individual responsibility to be cyber defenders. Protecting our networks must be ingrained in the organizational mindset at all levels. Culture change is hard, but with training, best practices, and your cooperation it can become second nature.

The 2023 NGA Cybersecurity Strategy—in conjunction with the 2020 NGA Technology Strategy, NGA Data Strategy 2021, and the 2023 National Cybersecurity Strategy—will be fundamental to reaching our envisioned end state of delivery of GEOINT supremacy, accelerated effects, and decision advantage.

The Cybersecurity Strategy within these pages reinforces the tenets of the NGA Strategy and provides the framework for achieving five cybersecurity goals:

1. **Advance Access Management**
2. **Deliver a Standardized, Secure Enterprise**
3. **Secure Data as a Strategic Asset**
4. **Lead with People**
5. **Evolve the Culture**

We keep our systems secure and mission operational when we all consider cybersecurity an essential part of our jobs.

VADM Frank D. Whitworth, USN
Director, NGA

Foreword & Introduction

Letter from the CISOs



NGA's cybersecurity strategy is, first and foremost, a means of realizing the Agency's GEOINT vision by keeping cyberspace safe and confronting various cyber threats to our missions. In addition, the strategy aims to ensure NGA is a leader in technological innovation and an active partner in shaping the cyber terrain. Alongside NGA's Technology and Data Strategies, this document will act as the third foundational pillar to ensure NGA achieves its cyber vision and is positioned for mission success.

In publishing this strategy, we recognize that NGA cannot improve cybersecurity in isolation, and that partnerships with businesses and community groups will continue to be required if we are to achieve success. We will need collaboration from across the enterprise—from the Office of Contract Services to Financial Management, Research and Development, Data and Digital Innovation, and more.

This strategy is the conceptual and practical foundation for achieving our goals, designed to efficiently structure the Agency's efforts and ensure a stable, long-term solution for the challenges arising in cyberspace. From performing basic cyber hygiene to deploying sophisticated deterrence, we will focus on raising the cost of mounting an attack against NGA and will hold aggressors at risk. With this strategy as our guide, we will now concentrate on the implementation plan for executing these fundamental goals.

NGA faces real and pervasive threats now. We must all embrace the individual responsibility to be cyber defenders if we are to succeed. Although it is crucial that we recognize our past accomplishments, we must reinvent our culture and approach to securing our greatest assets. This will not be easy. Our nation relies on us to defend NGA's GEOINT advantage today while evolving to meet the challenges of tomorrow. This is our call to arms where, together, we will secure the way.

Gary Buchanan
Chief Information Security Officer, NGA

Monica Montgomery
Deputy Chief Information Security Officer for Management and Strategy, NGA

Mike Ryan
Deputy Chief Information Security Officer for Compliance and Operations, NGA

Foreword & Introduction

Executive Summary

In the last decade, NGA has seen tremendous growth in the GEOINT discipline and the number of practitioners in industry, in academia, and at all levels of government.

As the GEOINT ecosystem has grown, so have its adversaries—who are persistent, adaptive, and often anonymous in cyberspace. To meet these threats, NGA will require a synchronized, cross-Agency approach.

Together, we will mindfully shape our cybersecurity efforts and continue to show the way. To do this, we will:

Enhance our access management and cross-domain services. NGA will support the ongoing shift to data-centricity and aim to securely get the right information to the right people at the right time.

Deliver a GEOINT enterprise that is secure and designed to higher standards. NGA will distinguish itself through improved risk management, zero-trust principles, and advanced defense tools.

Employ data as a strategic asset for decision-making. NGA will strengthen our use of artificial intelligence (AI), machine learning (ML), and computer vision (CV) in cybersecurity to identify patterns and threats, provide continuous monitoring, and speed the operational effectiveness of our enterprise.

Strengthen operations through people-driven cybersecurity. To bolster our future cybersecurity, NGA will communicate more transparently and comprehensively about cybersecurity, focus on recruiting and retaining cyber-savvy talent, and commit to increased cyber training for our workforce.

Redefine the culture of cybersecurity. NGA must reinvent its perspective on cybersecurity. As one team, we must understand that cybersecurity is no longer an IT challenge, but an Agency-wide business problem that we will face together.

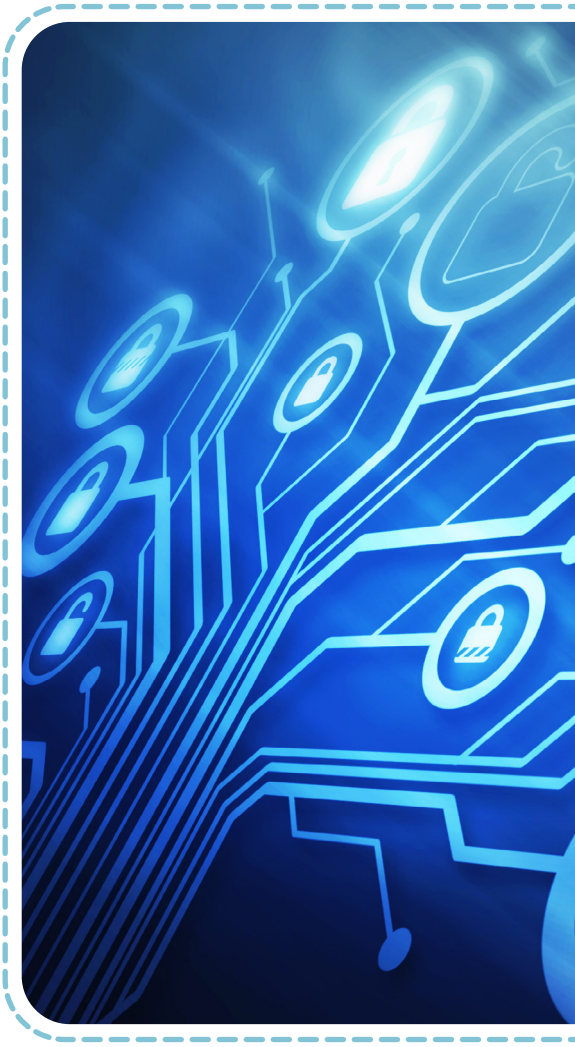

SECURITY
1024.256

- **Protect the people of NGA and our GEOINT enterprise by safeguarding critical infrastructure, workflows, and data through Federal Identity, Credential, and Access Management (FICAM).**

- To achieve the goal of advancement within access management, NGA must focus on two fundamental topics: FICAM and Cross-Domain Services (CDS).

- Multi-factor authentication (MFA) and fine-grain access control (FGAC) are critical elements of FICAM and achieving this goal. MFA secures access and data by requiring multiple login credentials. FGAC further secures access by allowing only users with mission needs to retrieve specific data and use specific systems. These two elements will yield an improved level of overall security, limit risk, enhance attribution, and expand control between interrelated programs.

  To further support the DoD shift to data-centricity, we will aim for improved location awareness for devices with access to NGA networks, such as laptops and mobile devices. In order to achieve greater governance and orchestration of a more secure operating environment and to facilitate data-driven decision-making, we must focus on location-specific services, enhanced machine identity management, and advanced data tagging.



- CDS is necessary to access or transfer data between multiple networks using different security classifications. It enables immediate and secure information-sharing with the right people at the right time, such as warfighters requiring GEOINT data to make real-time decisions.

- The areas of emphasis for CDS include "Raise the Bar" (RTB) compliance and full governance.
  - RTB is a set of cybersecurity standards designed to protect National Security Systems (NSS) by improving security and capabilities from design, development, assessment, implementation, and use perspectives.
  - Full governance of CDS and data flows helps enhance decision-making, manage policy, and improve enterprise efficiency through standardized, enterprise-level practices that help specific operations succeed.

- We are committed to working at the speed of mission, but it is critical to balance that speed with risk management.

- **Leverage and enforce IC, DoD, and industry standards to create an improved security posture through secure enterprise architecture, risk management framework, zero trust, and computer network defense.**

- A secure enterprise architecture is built on the inclusion of best practices in information technology (IT) security: from design to execution and, ultimately, decommissioning. We will start with the principles outlined in NGA's Technology Strategy and realized within the NGA Common Operations Release Environment (CORE), as we are guided by the tenets of the NGA Software Way.

Risk Management Framework (RMF)

RMF is a comprehensive, flexible, repeatable, and measurable process for organizations to manage information security and privacy risk for systems and organizations. It will provide NGA with continuous system and capability monitoring for timely notification and management of vulnerabilities, incidents, and potential threats.

Early, vigorous adoption of cybersecurity within the acquisition and system development lifecycle (SDLC) will enable NGA to deliver authorization to operate (ATO) at the speed of mission. Throughout, we will maintain the critical balance between speed and the risk-based approach required for successful implementation of security principles.

Zero-Trust Architecture

Implementing a zero-trust architecture—a security model that acknowledges threats exist both inside and outside the traditional network boundary—is a strategic approach to securing an organization's IT enterprise and digital user identities by removing the implicit trust between systems and users in favor of continuously reevaluating credentials at every digital interaction.

Computer Network Defense (CND)

The CND cybersecurity methodology uses computer networks to protect, detect, and react against a variety of cyber threats, which provides NGA's security architecture with multiple layers of defense. It also reduces our risk of attack or intrusion by aligning our technology components with the most effective policy, controls, and security management practices. This reduced risk yields lower costs for security integration, enhances identification and attribution of cyber perpetrators, and expands communication between interrelated programs and systems.

- **Obtain and use trusted, relevant data to make proactive cyber decisions across the Agency through data-driven decision-making; include AI, ML, and CV in business workflows; and mitigate risk through continuous authorization and continuous monitoring (CONMON).**

- Using data as a strategic asset starts with collecting the right data within the GEOINT pipeline. Using the principles of NGA's Data Strategy, we can adapt our security posture to address evolving global threats.

- **Data-Driven Decision-Making**

  Data-driven decision-making provides visibility into the enterprise by turning standardized, current security data into risk management insights that counter emerging threats and challenges. This process helps us identify security gaps through a comparison of risk vectors and supports informed security improvement plans across NGA. It also significantly improves visibility into business intelligence and how we can better incorporate unbiased data and program collaboration into the decision-making process.

- **AI, ML, and CV Within Cybersecurity**

  Analyzing past and current enterprise security data will enable us to predictively identify trends, patterns, and threats. Over time, these adaptive security measures will also enable us to automate many decision-making processes.

  Developing tools that integrate AI, ML, and CV into decision-making can help NGA manage large volumes of data and hasten our detection of and response to both routine and sophisticated multi-point threats. This will enable our workforce to engage in complex analysis more efficiently and improve the delivery of that analysis and other information to stakeholders.

- **Continuous Authorization to Operate (cATO) and CONMON**

  After a system or software is authorized or approved for use, cATO provides continuous discovery and monitoring of risk and external threats to a security environment—effectively integrating automation within system monitoring. Used together, these strategies strengthen the RMF and other NSS controls, and promote an effective shift to a data-centric model for real-time analytics and threat response.

- **Strengthen people-driven cybersecurity through training that reinforces collaboration and advances the cybersecurity tradecraft.**

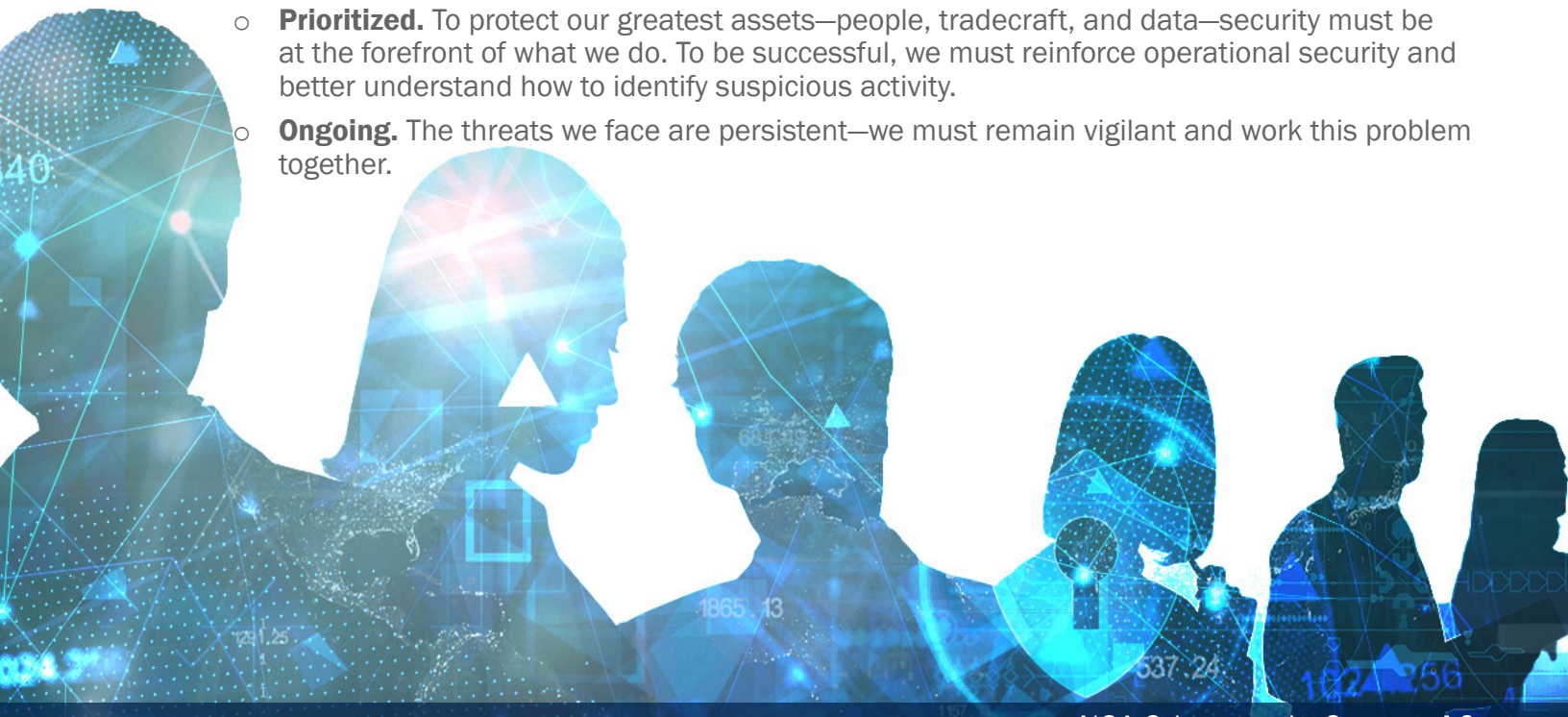
- Through leading-edge workforce training, community collaboration events, and focused awareness of changing cyber issues and practices, we will usher in a future that advances cybersecurity work roles at NGA, heightens talent recruiting and retention, raises cybersecurity awareness, and supports DoD 8140 policy series, which provides guidance for redefining and managing the cyber workforce.

- Supplying relevant workforce training provides cybersecurity consistency for NGA and its partners, increases the knowledge and scope of cyber roles, and lays the foundation for future cyber initiatives.

- As we develop a new cadre of cyber professionals, NGA will focus on continually improving our cybersecurity practices and related tradecraft.

- In addition to strengthening the knowledge and capability of our workforce, we will provide them with the technology necessary to secure our GEOINT advantage.

- To socialize and emphasize the importance of the cyber mission throughout the workforce, our message must be:
  - **Understandable.** We must clearly express how the cyber mission interacts across the enterprise in a manner that connects us all to GEOINT.
  - **Unified.** NGA and our partners have a stake in GEOINT security; we must face cyber threats together.
  - **Diversified.** We must improve how NGA communicates and shares the cyber mission so we can better connect our people to what they need to know.
  - **Prioritized.** To protect our greatest assets—people, tradecraft, and data—security must be at the forefront of what we do. To be successful, we must reinforce operational security and better understand how to identify suspicious activity.
  - **Ongoing.** The threats we face are persistent—we must remain vigilant and work this problem together.



- **Reach an Agency-wide understanding that cybersecurity is a shared responsibility, not simply an IT challenge.**

- Cybersecurity is more than an IT challenge—it is a business problem that requires an Agency-level focus. End-user security awareness is not enough to reduce our cybersecurity risks. We must heighten cybersecurity accountability and situational awareness—from start to finish—and strengthen community collaboration and partnerships within the GEOINT ecosystem.

- Successfully integrating cyber-accountability into our business practices will provide incentives for and promote the adoption of cybersecurity best practices and standardize them throughout the Agency. Increased collaboration with the Office of Contract Services on cybersecurity projects will help integrate cyber requirements within the acquisition process from the start. Enhancing the incorporation of cybersecurity into contracts is integral to maintaining the security standards that we set across our contracts, the bidder's library, and the entirety of NGA's enterprise. We must give security and mission requirements equal weight.

- The fight for a secure GEOINT enterprise cannot be won alone. We will collaborate more broadly with those who can help make a difference. Whether it is an Educational Partnership Agreement (EPA) that helps contribute to the curricula being taught to future cyber professionals or a Cooperative Research and Development Agreement (CRADA) to share hard problems and prepare for future acquisitions, our cyber efforts will expand the scope of collaboration.

- #SecureGEO is our initiative to lead the way in cybersecurity alongside the community and our partners. Expanded collaboration—such as CRADAs, EPAs, and Partnership Intermediary Agreements that we establish under our Title 15 authority—will strengthen how we integrate our strategic partnerships into acquisition. Focusing on tailored engagements will help stimulate community participation by improving our understanding of how we can align our efforts with industry and academia to achieve common goals and will aid in the development of cyber professionals who understand the GEOINT mission.

NGA
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

NGA.mil

Approved for public release, NGA-U-2023-02442