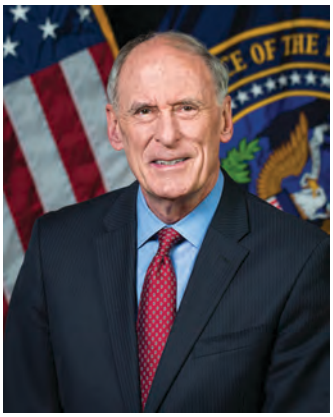
Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan

August 2019

ЩО-3
8,674
ЩО-4
9,222
ЩС-2
Ру=36,6кВт
Рр=34,7
Ip=60,16А
ЩС-2
Ру=36,6кВт
Рр=34,7
Ip=60,16А
ЩО3-Н-8,674-15-0,25-375-0,3
NYM-5x10 L=25м
ЩО4-Н-9,222-15-9-20-318-0,3
NYM-5x16 L=20 Т 32=4м
ЩО2-Н-36,6-60,16-6-360-0,3
NYM-5x25 L=10м
ЩО2-Н-36,6-60,16-6-360-0,3
NYM-5x25 L=10м
ЩО8505-0415
ЩО8505-0415
ЩО8505-0415
ЩО8505-0415
ДР 3-3093
ДР 3-3093
АЕ2046
Ip=100А
АЕ2046
Ip=40А
АЕ2046
Ip=100А
АЕ2046
Ip=40А
АЕ2046
Ip=40А

TABLE OF CONTENTS

Message from the Director of National Intelligence



Daniel R. Coats
Director of National Intelligence

We face a perfect storm comprised of information technology (IT) vulnerabilities associated with the proliferation of software and network technologies; increasing reliance on foreign-owned, manufactured, or controlled hardware, software, and services; and adversaries' increasingly persistent and sophisticated asymmetric cyberattacks. Their focus – United States (U.S.) Government agencies; academic and research institutions; our critical infrastructure; and commercial enterprises in the U.S. IT supply chain. Adversaries strive to outpace us in advanced technology, render our technologies unreliable, and steal our intellectual property.

The increased and pronounced ransomware attacks, massive data breaches, and supply chain attacks in the commercial sector are disturbing trends that very possibly could infiltrate our secure IT environments. Recent compromises of managed service providers and legitimate software allowed cyber adversaries to cause large-scale disruptions to U.S. infrastructure. In response to these events, the President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, on 11 May 2017, requiring the federal government to enhance its agility to detect, understand, characterize, and share information about cyber threats supporting national security decision making.

As an Intelligence Community (IC), we must collectively improve our cybersecurity posture and enhance our cyber defenses to ensure the security of our intelligence networks and systems. Each IC element must recognize its role in a secure, connected, data-centric, integrated, and transparent technology environment in which shared cybersecurity intelligence benefits the entire enterprise.

This plan for improving IC cybersecurity constitutes collaboration between the Office of the Intelligence Community Chief Information Officer, National Counterintelligence and Security Center, National Intelligence Manager – Cyber, Intelligence Community Security Coordination Center, and all 17 members of the IC. We appreciate your participation and continued engagement.

The Director of National Intelligence shall oversee IC element information security policies and practices, including:

(1) Developing and overseeing the implementation of policies, principles, standards, and guidelines on information security;

(2) Requiring [IC elements] to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintains by or on behalf of an [IC element]; or information systems used or operated by an [IC element] or by a contractor of an [IC element] or other organization on behalf of an [IC element].

*Federal Information Security Modernization Act (FISMA) of 2014 §3553

Message from the Intelligence Community Chief Information Officer and Intelligence Community Chief Information Security Officer

John B. Sherman
Intelligence Community
Chief Information Officer

The IC is undergoing unprecedented transformation. Managing a fluid geopolitical environment requires the IC to be agile in delivering IT systems and thoughtful in sharing intelligence information. IC elements continue to find new ways to collaborate, coordinate, and share information across agencies and with non-traditional partners. Modernizing the IC's IT infrastructure enables this transformation and leverages increasingly sophisticated technology.

The rapid assimilation of new services, software, and raw and finished intelligence products are dramatically changing the way the IC needs to safeguard its data. As the mission expands, the IC needs to understand and respond to the holistic risk presented by operating in the same interconnected cyber environment that our adversaries target. For this reason, we must unite in securing the Intelligence Community Information Environment (IC IE).

Meeting the objectives detailed in this plan requires unprecedented partnership and understanding among senior leadership; cyber, cybersecurity and IT professionals; mission leadership; program managers; acquisition executives; supply chain and cyber threat analysts; and counterintelligence experts. We are excited at the opportunity to engage with the Community to work on such an important initiative.

Susan T. Dorr
Intelligence Community
Chief Information
Security Officer

*The Director of National Intelligence has authority over systems that are operated by an [IC element], or another entity on behalf of an [IC element] that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an [IC element].**

*Federal Information Security Modernization Act (FISMA) of 2014 §3553

The IC CIO is responsible for developing and overseeing the implementation and IC element adoption of policies, principles, standards and guidelines on information security promulgated for national security systems as authorized by law and directed by the President and to identify and provide information security protections commensurate with risk consistent with the information security requirements established by Subchapter III of FISMA.

**Intelligence Community Directive 500

PURPOSE

This implementation plan establishes a framework of cybersecurity objectives and tasks where IC elements can focus their limited resources to address modern threats and mitigate the highest risks to the IC IE

BACKGROUND

Safeguarding the Intelligence Community Information Environment (IC IE) is a fundamental component of the National Intelligence Strategy. Per law, order, regulation, and policy, all 17 elements of the Intelligence Community (IC) must secure and protect the people, information, and enterprise, mission, and business information technology (IT) that are so vital to intelligence mission success.

On 12 February 2018, the Principal Deputy Director of National Intelligence (PDDNI), Susan Gordon, directed the Intelligence Community Chief Information Officer (IC CIO) to develop this plan in collaboration with IC elements and other components of the Office of the Director of National Intelligence (ODNI) in response to:

- A series of recent unauthorized disclosures;
- Multiple annual IC element Chief Information Officer (CIO) and Inspector General Federal Information Security Modernization Act (FISMA) reports indicating deficiencies in managing and maintaining vulnerability management (VM) programs and basic computer hygiene; and
- A National Intelligence Council Memorandum issued in December 2017 that highlighted the top cyber risks and threats to the intelligence mission.

The intent of this implementation plan is to:

- Identify the fundamental, common, and maturing tasks of greatest importance to safeguard the IC IE;
- Raise awareness of the various roles and authorities across the elements that must collaboratively engage in executing IC IE cybersecurity activities; and
- Foster ongoing conversations about enterprise security risks and the balance of investment and sustainment to mature the IC IE safeguarding posture.

*The IC IE includes the individuals, organizations, and IT capabilities that collect, process, or share Sensitive Compartmented Information (SCI), or that, regardless of classification, are operated by the IC and are in whole or in majority funded by the National Intelligence Program.**

*Intelligence Community Directive 121, Managing the Intelligence Community Information Environment

INTRODUCTION

Our adversaries are actively attempting to exploit cyberspace. The IC's dynamic IT environment provides unique cybersecurity challenges in countering this threat landscape. There are numerous facets to responding to our adversaries efforts, both offensive and defensive.

This Implementation Plan focuses on safeguarding the IC IE through the disciplines of routine computer hygiene, asset and configuration management, and cybersecurity. Several of these are included as guidance to IC elements in the *Consolidated Intelligence Guidance Fiscal Years 2021-2025*, recently signed by the DNI and USD(I). According to the National Initiative for Cybersecurity Careers and Studies, cybersecurity is the "activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

The most significant efforts towards defending the IC IE should focus on the fundamental cybersecurity principles listed below. Industry thought leaders, such as the SANS Institute, indicate that organizations can mitigate over eighty percent of cybersecurity vulnerabilities by performing basic computer patching and hygiene. This requires mature and comprehensive efforts to know, manage, and share the state of the enterprise, including all enterprise, business, and mission IT.

Fundamental Cybersecurity Principles

Know your enterprise

Maintain a complete inventory of all enterprise, mission, and business hardware and software, coupled with network maps, topologies, and data.

Manage your enterprise

Keep hardware and software current by installing security patches, updating software, and upgrading old or deprecated hardware and software. Harden operating system configurations per standards. Execute routine computer hygiene to identify deficiencies.

Share the state of your enterprise

Share agreed-to data, key performance indicators, and event metrics that support the IC IE's overall health and security status. Openly report and provide this data to the IC Security Coordination Center for correlation and management of a holistic and shared IC cybersecurity situational awareness.

While these fundamental principles provide basic security, they are insufficient to address the full scope of threats. The IC must leverage complementary security disciplines, to include human, physical infrastructure, and technological, to ensure end-

to-end safeguarding. Additional activities currently underway, such as maturing supply chain processes, articulating data protection requirements, and reducing unauthorized disclosures significantly contribute to holistic efforts to manage risk.

IC elements are improving their respective security postures; however, these efforts do not address the IC IE's connected nature and only marginally improve the enterprise. The *Consolidated Intelligence Guidance (CIG) for Fiscal Year (FY) 2020-2024* highlights this realization, "IC elements must resolve long-standing barriers to successful implementation of a shared secured information environment in which all elements participate and proactively protect for the benefit of integrated intelligence mission operations."

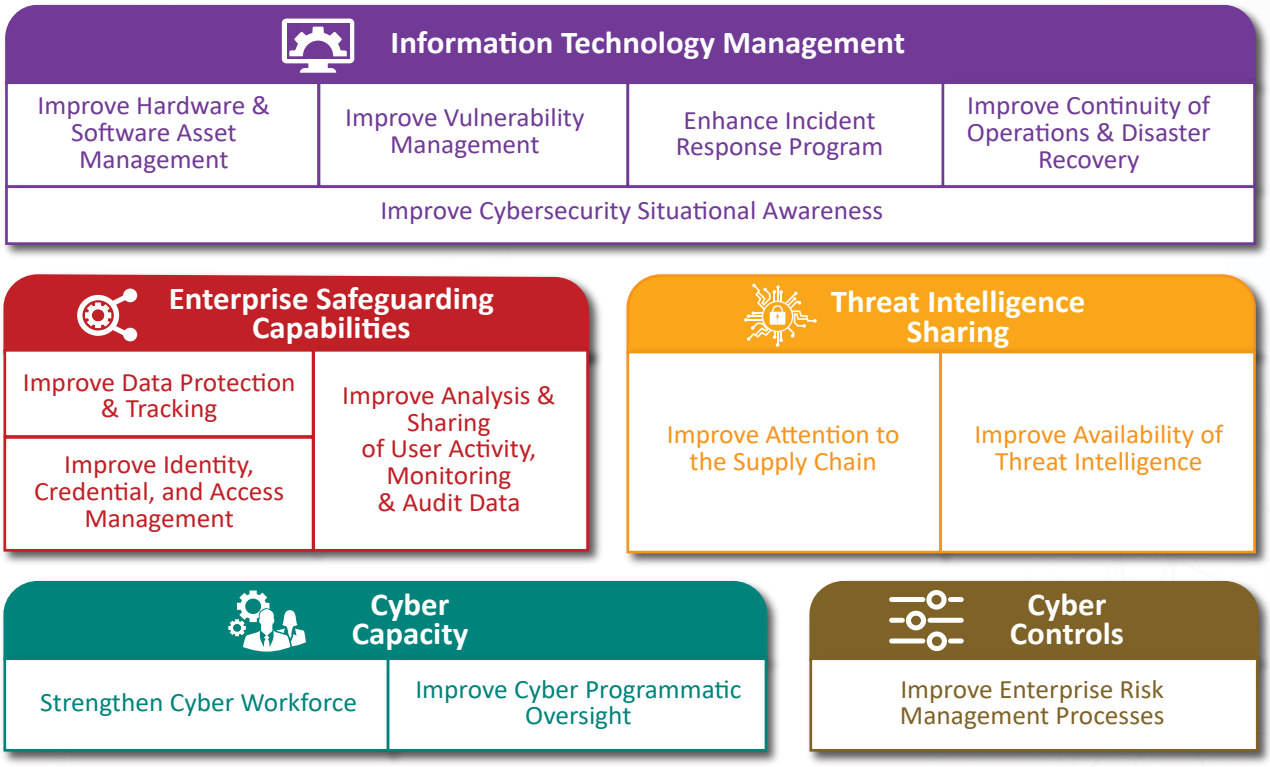
This Implementation Plan identifies a number of objectives and tasks for improving the cybersecurity of the IC IE, while balancing risk tolerance against mission delivery. The IC must augment and leverage existing capabilities, expertise, and insights as a collective body to defend against advanced persistent threats.

Key Implementation Plan Assumptions

- ***Scope*** – All enterprise, business, and mission IT assets, data and datasets, both classified and unclassified, including IT assets associated with U.S. information systems and partnership information systems (as defined in IC Standard 503-04, *Managing Non-U.S. Personal Access to Information Systems*) and those that cross network security boundaries.
- ***Agreement*** – The IC collectively agrees on a set of cybersecurity initiatives against which resource tradeoffs with mission capabilities must be made.
- ***Collaboration*** – The IC will collaborate on solutions and areas of common interest to enhance IC IE cybersecurity.
- ***Technology*** – The IC will adopt and integrate advanced technology (e.g., artificial intelligence/machine learning) necessary to predict and identify threats and proactively mitigate vulnerabilities.
- ***Maturation*** – The IC will adjust strategy, policy, and budgets in response to maturing technologies and processes.
- ***Management*** – The IC will normalize fundamental and repeatable aspects of IT management across the IC for both reporting on cybersecurity performance status and responding to occurring threats.
- ***Strategy*** – The IC will develop a higher order cybersecurity strategy to respond to the National Intelligence Strategy and CIG strategic outcomes, while driving this Implementation Plan.
- ***Workforce*** –The IC will identify, expand, recruit, develop, retain, and sustain a cybersecurity workforce with the knowledge, skills, and abilities to respond to cybersecurity challenges.

FUNCTIONAL FRAMEWORK

The IC Chief Information Security Officer (IC CISO) and IC element CISOs identified thirteen objectives spanning five functional areas.



IC Cybersecurity Implementation Plan Functional Framework

These objectives emphasize recurring themes identified by IC elements in annual FISMA and *Integrated Defense of the IC Information Environment* reporting. The CISOs identified these objectives as the most relevant items to reduce cybersecurity risks and achieve an improved and mature IC IE.

Key interdependencies exist between the thirteen objectives. For example, *Improve Attention to the Supply Chain* requires secure, standardized processes and architecture that ensures the integrity of vendor software updates to *Improve Vulnerability Management*.

FUNCTION: INFORMATION TECHNOLOGY MANAGEMENT

Managing information technology is a joint responsibility of IT and security professionals. Cybersecurity responsibilities extend throughout the organization, possibly to individuals in roles not accustomed to thinking of themselves as part of the security practice. From the cybersecurity perspective encompassed in this plan, security professionals include not only the typical information systems security engineers and operators, but also business professionals, such as program managers (PMs) and acquisition executives, who all must take active roles in the larger organizational and enterprise safeguarding objectives.

Performing basic hardware and software asset management is critical to understanding and measuring improvements in an organizational cybersecurity baseline and safeguarding posture. Preventing exploits against known vulnerabilities within and among known and managed IT assets is imperative. Performing proactive prediction, identification, and response to security incidents happening to known and managed IT assets is critical to limiting potential damage. Continuing to operate or recover known and managed IT assets during and after natural disasters or cyberattacks ensures mission performance during extreme circumstances. Maintaining IC-wide cybersecurity situational awareness of vulnerabilities to and events against known and managed IT assets, as well as our response to human or natural threats to operations, keeps IC leadership and security professionals as a collective whole in a continuous state of preparation, response, and informed decision-making.

FUNCTION: ENTERPRISE SAFEGUARDING CAPABILITIES

Fundamental to the IC's secure cloud services architecture is the concept of "tag the data, tag the people, and audit user and system activities." Maintaining data and information that is known, standardized, and self-describing with metadata for discovery, access rights, and handling postures IC data holdings for maximum discovery and appropriate access and retrieval. Providing a common, sharable

method for managing identities, attributes, and entitlements for person entities and non-person entities enables access decision systems to grant users and systems appropriate access to data and other systems. Auditing user and system activities and feeding event data to and alerting appropriate individuals responsible for monitoring malicious behavior and performing counterintelligence functions provides an important aspect of IT monitoring for unauthorized disclosures and intentional threats.

Implementation of these architectural and engineering approaches at both the organizational and enterprise levels continues to be a work in progress, with enabling mission and business systems remaining a significant challenge. The IC is federating solutions across the enterprise to provide consistency across all IC users and systems. The Intelligence Community Chief Data Officer collaborates with IC element Chief Data Officers (CDO) to advance common data reference architectures, standards, and data management practices, and data services to posture IC data holdings for data science and augmented intelligence. However, inconsistent implementation of these approaches will increase data protection gaps and vulnerabilities within the enterprise, thereby increasing the efforts across other plan objectives to mitigate security risks.

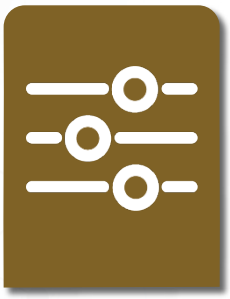
FUNCTION: THREAT INTELLIGENCE SHARING

Adversaries continue to enhance their cyber capabilities to compromise sensitive information, alter data, and disrupt or destroy systems. The President's 11 May 2017 Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, called upon the Federal Government to enhance its agility to detect, understand, characterize, and share information about cyber threats in support of enabling comprehensive security risk decision-making.

This function focuses on two primary forms of threat intelligence that feed the *Information Technology Management* and *Cyber Control* objectives. Intelligence regarding supply chain threats and other cyber threat actors is critical to informing cyber defensive preparations and response, as well as, program management and acquisition decisions.

FUNCTION: CYBER CAPACITY

A successful cybersecurity program recognizes the cross-functional nature in securing and safeguarding our information systems. Program management, acquisition, and software/systems development all must address security early and throughout the lifecycle, and continuously monitor IT operations.



FUNCTION: CYBER CONTROLS

Enterprise-level risk management enables IC leaders to set priorities and direct resources towards mitigating vulnerabilities and reducing the threat landscape. Improving the IC's approach to enterprise risk management requires proactive engagement to stay ahead of the threat. A full appreciation and understanding of enterprise risk activities, such as Risk Management Framework processes, are integral to becoming agile and transparent within the development life-cycle. Ongoing security assessments such as those conducted by blue and red teams are a key activity in managing the IC IE's operational security posture. Central to effective risk management is timely, comprehensive information sharing across the IC and with partners in federal government, the Defense Industrial Base (DIB), and private sectors associated with the nation's critical infrastructure.

OBJECTIVES AND TASKS

The thirteen objectives detailed in the following pages are mapped to activities defined in the *FISMA of 2014*. Each objective also contains a strategic outcome, contextual description, and the required tasks and champions necessary to address IC shortcomings in protecting the IC IE. The IC CISO and IC element CISOs simultaneously identified these tasks and objectives. Many tasks include a source which are numerically identified by "[ ]" and listed in Appendix A.

The objective tasks are organized into three groups:

- **Green** – Fundamental activities critical to improving routine computer hygiene and IT management improving the IC IE's basic security posture. IC elements are responsible for completing these tasks.
- **Yellow** – Common processes and standards to close the gaps in guidance or to enable shared cybersecurity capabilities. These tasks are largely the purview of ODNI components or IC elements to lead or provide as IC IE-wide capabilities.
- **Blue** – Maturing activities that improve enterprise efficiencies over time. IC elements and ODNI components share responsibility to perform.

NIST CSF

The *Cybersecurity Enhancement Act of 2014* statutorily expanded NIST's role to better address risks to include identifying and developing cybersecurity risk frameworks for use by critical infrastructure owners and operators. NIST was required to identify "a prioritized, flexible, repeatable, performance-based and cost effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." NIST created the CSF in response to this guidance. Executive Order 13800 further emphasized the priority for federal agencies to align to the NIST CSF. The NIST CSF consists of five concurrent and continuous functions – Identify, Protect, Detect, Respond, and Recover.

FISMA of 2014, 44 U.S.C §3554 (b)

IC elements are to develop, document, and implement organization-wide information security programs to secure the information and information systems that support operations and organizational assets, including those provided or managed by another element, contractor, or other source. IC element information security programs are to include:

1. Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets the element.
2. Policies and procedures that are based on periodic risk assessments; cost-effectively reduce information risks to an acceptable level; ensure that information security is addressed throughout the life-cycle of each element information system; and ensure compliance with applicable requirements, policies, procedures, and guidelines.
3. Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate.
4. Security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the element, of information security risks associated with their activities; and their responsibilities in complying with element policies and procedures designed to reduce these risks.
5. Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing shall include testing of management, operational, and technical controls of every information system identified in the inventory.
6. Process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the element.
7. Procedures for detecting, reporting, and responding to security incidents, which shall include mitigating risks associated with such incidents before substantial damage is done.
8. Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the element.

IMPLEMENTATION

This plan provides a starting point for improving cybersecurity. It can only be achieved if IC leaders understand and commit to the resources, time, and scope of this endeavor. Deputy Directors of IC elements are responsible for informing the PDDNI of conflicts or impediments encountered in implementing this plan.

IC elements should develop Intelligence Program Budget Submissions and prioritize investments to achieve the strategic objectives and tactical activities presented here. IC element CIOs should convey to PMs how their respective programs align to these tasks by FY.

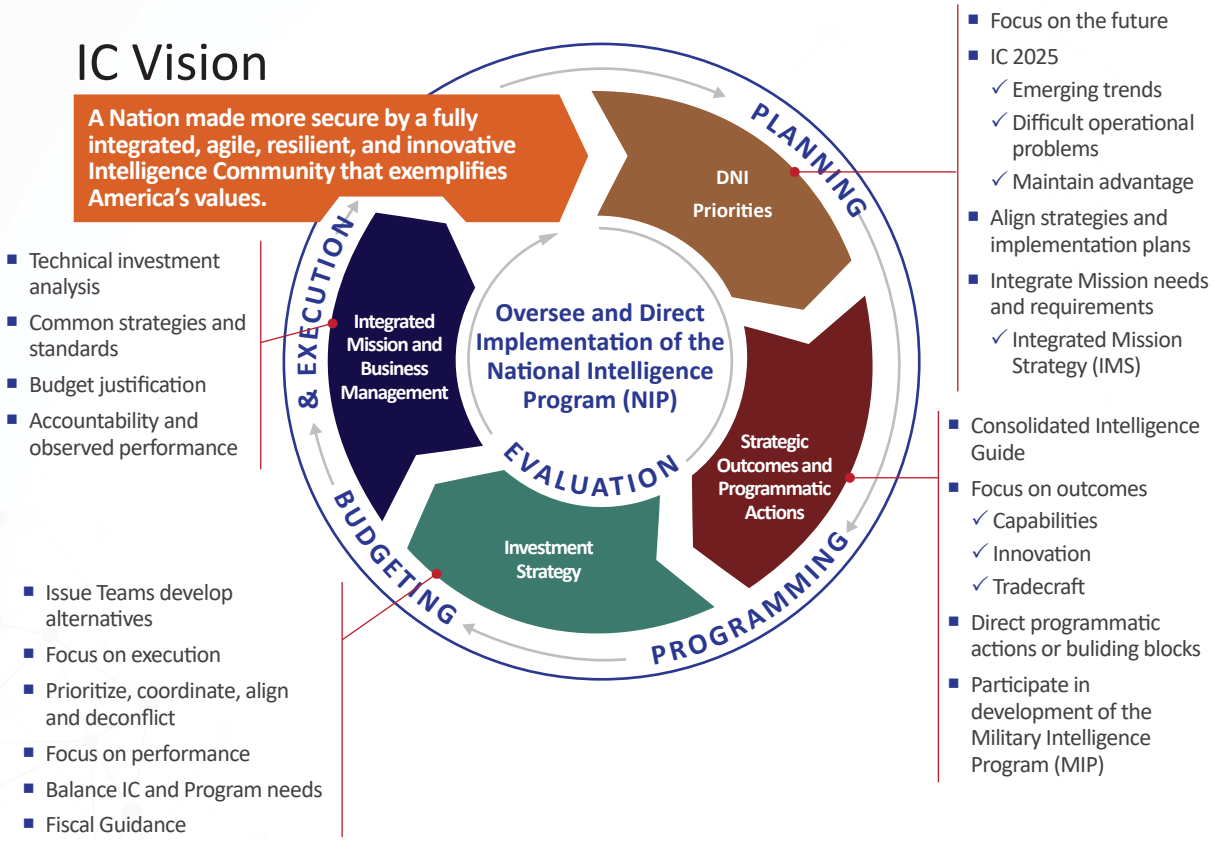
The IC CIO intends to follow a defined process to oversee execution of this plan. In July 2018, the PDDNI, IC element deputies, and CIOs agreed to the initial selection of eight high priority tasks determined by the IC element CISOs (see Appendix B). The IC CIO intends to prioritize execution of the subsequent tasks through the following criteria:

- **Monitor** – Measure performance using the IC IE Cybersecurity Performance Evaluation Model (CPEM) as a reporting mechanism to inform the PDDNI and IC element deputies of progress and to identify recommended actions.
- **Inform** – Leverage an array of sources such as IC policy, IC IE security risk assessments, enterprise architecture frameworks, agreed-to design patterns, and technical implementation guides.
- **Govern** – Tasks will be proposed to the IC element deputies yearly through appropriate governance and oversight forums and processes.
- **Plan** – Drive balanced and effective resource decisions aligned to IC element budget cycles.

The second set of priority groupings will initially address the comprehensive completion of the foundational IT management objectives, *Improve Software and Hardware Asset Management* and *Improve Vulnerability Management*, coupled with strategic implementation of other related tasks from other objectives (see Appendix B).

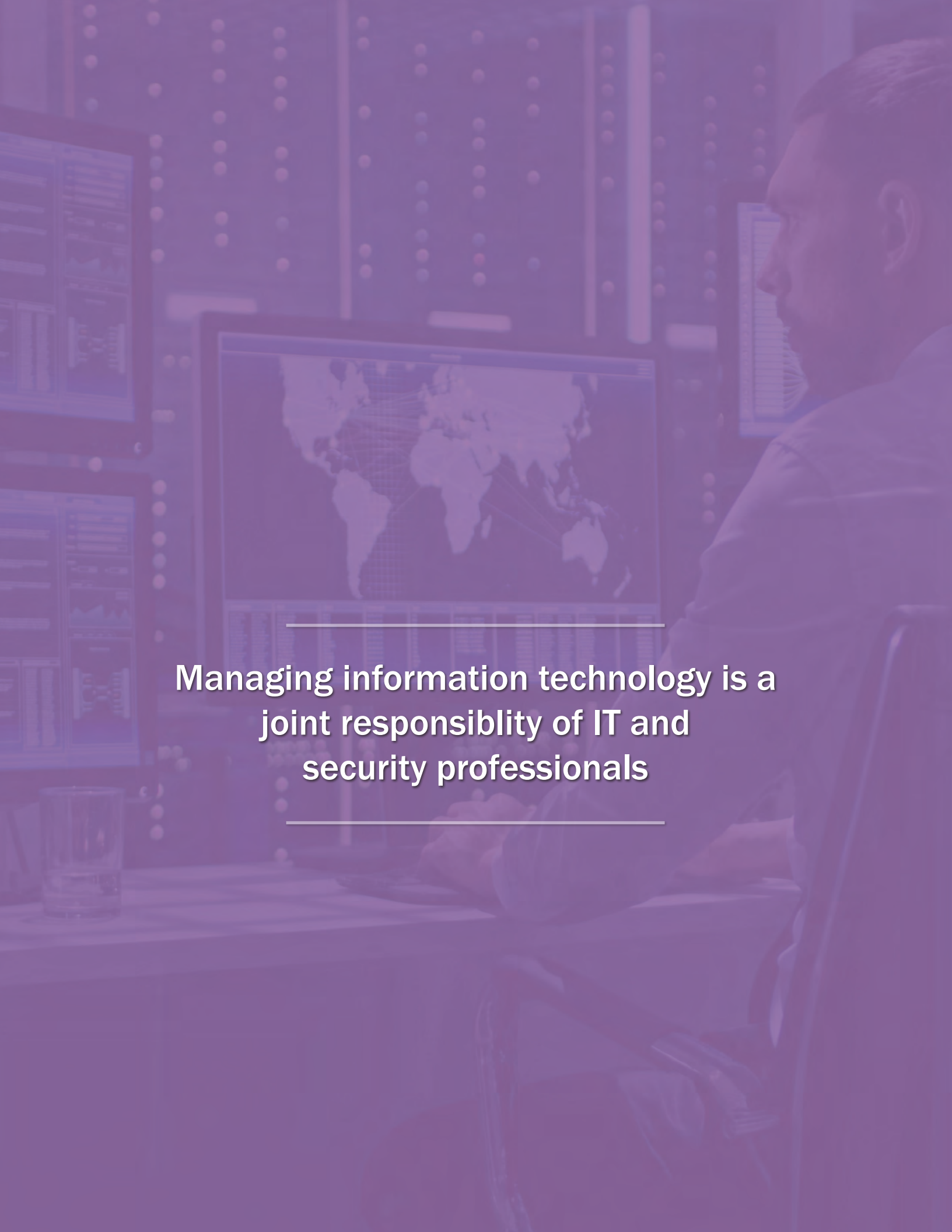
The ODNI will include prioritized tasks yearly via the formal CIG to ensure IC elements are addressing funding requirements through their yearly and five-year budget builds. Additionally, the ODNI will insert supporting guidance language into the Congressional budget guidance leveraging the ODNI Consolidated Resource Investment process.[1]

[1] Nothing in this plan is intended to impair or otherwise affect the authorities and obligations of the elements under applicable law, regulations, or directives; and performance of tasks must be in accordance with an element's repsective authorities.



A single IC effort to invest in capabilities that provide advantage

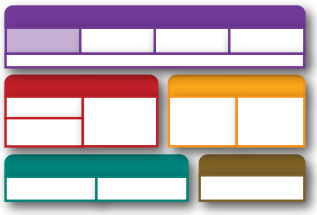
ODNI Consolidated Resource Investment Process



Managing information technology is a joint responsiblity of IT and security professionals

INFORMATION TECHNOLOGY MANAGEMENT

- Improve Hardware and Software Asset Management
- Improve Vulnerability Management
- Enhance Incident Response Program
- Improve Continuity of Operations and Disaster Recovery
- Improve Cybersecurity Situational Awareness



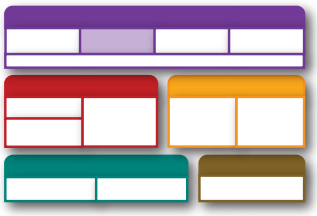
Improve Hardware and Software Asset Management

Strategic Outcome
Each IC element implements a Total Asset Management program to identify and manage all of its baseline IT (assets and connectivity) and data.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic testing and evaluation of effectiveness

Knowledge of an organization's IT assets and understanding how they are connected is the foundation for determining risks and making informed decisions. Managing the IT environment first requires identifying all IT assets, understanding how those assets are connected, monitoring them for configuration changes, and sharing that information with stakeholders. Network topologies are useful for understanding external communications.

Improving Hardware and Software Asset Management

	Tasks	Champion
Fundamental	1. Identify physical devices, systems, software platforms, and applications within the organization, to include Cross Domain Solutions (CDS). [1]	• IC elements
	2. Identify and map organizational communication and data flows and external information systems to which organization systems connect or use. [1]	
	3. Develop change control processes, supporting tools, and analytics to detect configuration changes. [1]	
	4. Identify High Value Assets (HVA) (i.e., NIST-defined High Impact systems, ICD 118, IC CIO Memorandum 2016-0072) and critical system architecture. [6]	
	5. Harden all Information Technology assets per common hardening guides (i.e., CIS Benchmarks, DISA STIGs, and NSA Hardening Guides). [1]	
	6. IC IT Asset Managers coordinate with their IC element's Total Asset Management Program Managers (PM) to incorporate the IC Acquire-to-Retire business process framework to manage IT assets.	
Common	7. Identify asset management tools and establish Enterprise License Agreements (ELA), where appropriate for IC use.	• IC CIO • ODNI/AP&F
Maturing	8. Integrate hardware and software asset management with an authorization database to identify when assets are added, removed, or modified thereby affecting the system's authorization status.	• IC elements • IC CIO



Improve Vulnerability Management

Strategic Outcome
Each IC element implements a program to monitor and remediate or mitigate known vulnerabilities.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic testing and evaluation of effectiveness ▪ Process for remedial action ▪ Procedures for security incidents

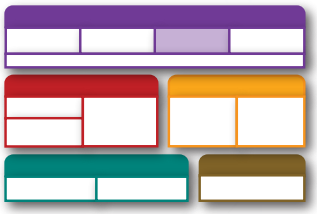
Vulnerability Management is a proactive practice designed to prevent exploitation of known vulnerabilities within an organizations' IT infrastructure. A formal VM program is necessary to manage existing vulnerabilities against ongoing threats and to prevent, to the degree possible, introducing new vulnerabilities into the environment. A successful VM program requires a robust asset management initiative so those individuals responsible for addressing vulnerabilities know all of the IT assets that are at risk.

The single highest attack vector adversaries exploit is through persistent vulnerabilities resulting from not patching or upgrading operating systems. Managing and regularly applying vendor-issued, critical software and security updates and patches increases the protection of data and systems from malicious attacks and erroneous function.

A mature organizational VM program consisting of repeatable and consistent processes, a regular maintenance schedule, and supporting operating procedures should reduce the overall number of known vulnerabilities across the IC IE. Additionally, phasing out unsupported hardware and software platforms and decommissioning old applications and systems no longer necessary or that have been replaced also significantly reduces risk, especially in large, unclassified, Internet-connected environments.

Improving Vulnerability Management

	Tasks	Champion
Fundamental	9. Implement a comprehensive hardware, software, and firmware vulnerability management process. [1] [2] [3]	• IC elements
	10. Eliminate end-of-life and unsupported hardware, software, and firmware. [3]	
	11. Increase Common Vulnerability Enumeration remediation rate to 95% or above. [3]	
	12. Implement automated, credentialed scans. [3]	
	13. Implement a VM process for those devices that are not reachable via the automated vulnerability management capability. [3]	
Common	14. Establish authoritative IC repository(ies) for approved software, firmware, and patches. [3] ***NOTE:*** *Optional for IC elements that desire to establish and maintain an internal organizational authoritative repository.*	• IC CIO • IC SCC • IC elements
	15. Establish authoritative, secure channel(s) or process(es) for moving approved software, firmware, and patches from low to high and checking availability of downloads from the IC repository. ***NOTE:*** *If IC element decides to maintain its own authoritative repository, this task must be met at the IC element level.*	
	16. Establish IC policies and recommended contract language requiring vendors to meet IC hygiene objectives, patching standards, and periodicity terms.	• ODNI/AP&F • IC CIO
Maturing	17. Use authoritative IC repository(ies) to obtain IC-approved operating system and software patches. [3]	• IC elements



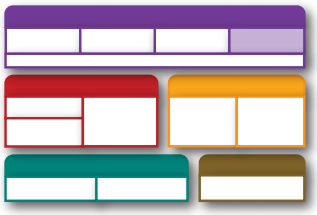
Enhance Incident Response Program

Strategic Outcome
Each IC element is actively managing its Incident Response Program to instinctively and collaboratively respond to cyber incidents.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic testing and evaluation of effectiveness ▪ Plans for continuity of operations ▪ Procedures for detecting, reporting, and responding to security incidents

Incident Response (IR) is the ability to proactively identify and respond to events that might negatively influence an IC element's mission requirements and may affect the IC as a whole. The response can vary depending on IT assets affected and the type of event. A successful IR program requires coordinated reporting and information sharing, both vertically within an organization and horizontally across the IC IE.

Enhancing Incident Response Programs

	Tasks	Champion
Fundamental	18. Test Incident Response plans annually either within the organization or as part of annual ICE STORM exercises. [5]	• IC elements
	19. Ensure monitoring and response services are available to detect and respond to all categories of incidents across the IC IE at all times.	
	20. Develop procedures for sharing incidents, response steps, and mitigation steps with CI organizations. [5]	
	21. Share guidance and information with the IC SCC on the steps taken to mitigate threats and impacts from events and incidents, to include intrusion detection signatures, adversary indicators, and incident mitigation procedures. [5]	
	22. Ensure procedures are available to leverage resources from and share threat and incident information with internal law enforcement, network management, CI, and federal government cyber partners housed within the IC element. [5]	
Common	23. Establish event and incident response guidance to include details for IC SCC reporting. [5]	• IC CIO
Maturing	24. Drive to near-real time incident response-based machine augmentation.	• IC elements



Improve Continuity of Operations & Disaster Recovery

Strategic Outcome
IC elements can rapidly and effectively recover and reconstitute IT functions to continue degraded or disrupted operations.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic testing and evaluation of effectiveness ▪ Plans and procedures to ensure continuity of operations

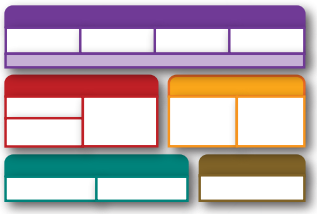
An IC element's Continuity of Operations and Disaster Recovery (COOP/DR) plan defines the organization's ability to continue IC missions during emergencies, including acts of nature, accidents, and cyberattacks. The goal is to ensure the workforce performs effectively when activating a COOP/DR response.

The growth of ransomware and destructive malware has dictated a greater need for the IC to exercise this capability. IC elements should strive for cyber sustainability and resiliency for all systems. However, recognizing that this can be costly, IC elements must perform necessary continuity and disaster recovery planning to align their security-designated High Value Assets with their COOP-defined mission-critical and mission-essential functions. This synchronizes the two disciplines to respond when:

- Establishing COOP/DR teams and assigning roles
- Establishing alternate work locations
- Testing COOP/DR plans and conducting exercises
- Activating COOP/DR plans, when necessary

Improving Continuity of Operations and Disaster Recovery

	Tasks	Champion
Fundamental	25. Identify all HVA IT assets as Mission Critical Function (MCF), Mission Essential Function (MEF), and ensure they are included in Continuity of Operations plans. [5] [6]	• IC elements
	26. Maintain situational awareness of operational capabilities and capacity of IT designated for IT continuity.	
	27. Conduct system contingency tests, training, and exercises at least annually. [6] [7]	
	28. Exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. [7]	
Maturing	29. Mature continuity planning, provisioning, installing, and testing of resilient, interoperable IT at IC facilities designated for IC continuity.	• IC elements



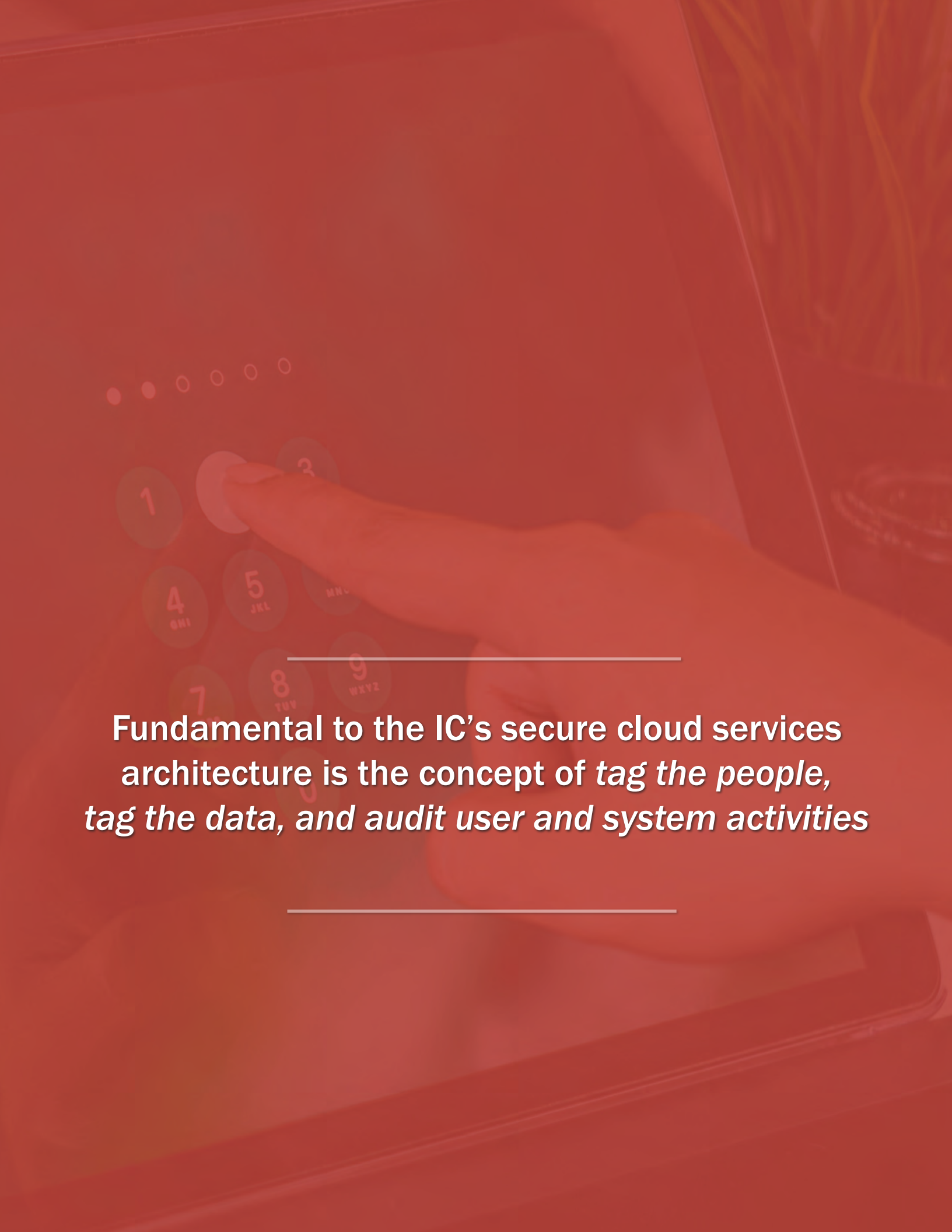
Improve Cybersecurity Situational Awareness

Strategic Outcome
IC elements automatically share with the IC Security Coordination Center (IC SCC) near-real time intelligence about cybersecurity to enhance IC-wide situational awareness and the ability to defend the enterprise.
FISMA Activity
▪ Subordinate plans for information security ▪ Procedures for detecting, reporting, and responding to security incidents

IC leaders need to possess a holistic understanding of IC IE cyber defenses and be able to make risk-informed, mission-impactful decisions in response to specific threats and vulnerabilities. To accomplish this, IC elements must share information about threats, vulnerabilities, mitigations, audit data, and risk decisions with one another. Collectively, this constitutes the body of knowledge by which IC leaders can share timely, relevant, and accurate operational assessments; jointly assume assessed consequences across the environment; and take action to defend against and respond to increasingly large-scale sophisticated attacks.

Improving Cybersecurity Situational Awareness

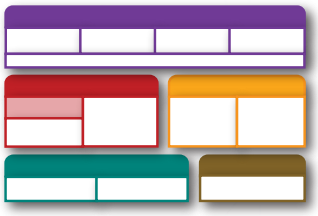
	Tasks	Champion
Fundamental	30. Provide automated Defense Information Systems Agency (DISA) Asset Summary Reporting (ASR) and Asset Reporting Format (ARF) summary reports to the IC SCC. [2] [10]	• IC elements
	31. Share with the IC SCC select information about identified IT assets and communication and data flows between internal and external information systems, to include cross domain solutions.	
Common	32. Establish common model and associated sharing agreements for threat warnings that leverage intelligence reporting.	• NCSC • CTIIC • ODNI/NIM-Cyber
	33. Establish Enterprise License Agreements (ELAs) for cyber capabilities (e.g., vulnerability scanning, end-point security, situational awareness, and threat intelligence monitoring services) widely used across the IC.	• ODNI/AP&F
	34. Establish an authoritative repository of intrusion detection system signatures.	• IC SCC
	35. Expand IC SCC counterintelligence (CI) and computer network defense (CND) assignee program across all IC elements.	
Maturing	36. Create IC cyber innovation program to research, evaluate, pilot, and report on emerging cybersecurity technologies (e.g., Artificial Intelligence, Machine Learning, Behavior Modeling, Executable Whitelisting, Security Operations Center Automation) to assist in threat identification and mitigation.	• IC elements
	37. Establish a mechanism for offensive cyber to proactively inform defensive threat mitigation activities.	• ODNI/NIM-Cyber
	38. Leverage Security Information and Event Management (SIEM) services and artificial intelligence (AI) to alert incident response teams of events that require human investigation and remediation.	• IC SCC
	39. Integrate disseminated cyber threat reporting to illuminate adversaries' activity and intentions advancing indications and warnings for the cybersecurity community.	• CTIIC



Fundamental to the IC's secure cloud services architecture is the concept of *tag the people, tag the data, and audit user and system activities*

ENTERPRISE SAFEGUARDING CAPABILITIES

- Improve Data Protection and Tracking
- Improve Identity, Credential, and Access Management
- Improve Sharing and Analysis of User Activity Monitoring and Audit Data



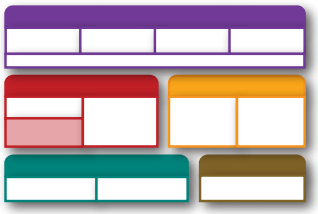
Improve Data Protection & Tracking

Strategic Outcome
Each IC element has identified and is managing all data assets according to defined data protection requirements.
FISMA Activity
▪ Subordinate plans for information security

Information moves rapidly through the IC IE and ultimately resides in commingled, shared repositories for discovery and analytics. IC elements responsible for specific types of information have functional authority for determining the protections required. IC element CISOs and Authorizing Officials must collaborate with functional managers, National Intelligence Mission Managers, and IC element CDOs to identify, establish, and register data protection requirements for which they are responsible. Producers want to trust that shared information is managed and protected regardless of physical or virtual location, or system.

Improving Data Protection and Tracking

	Tasks	Champion
Fundamental	40. Identify data assets within the organization. [1]	• IC elements
	41. Register datasets in the IC Catalog.	
	42. Prepare and condition datasets in conformance with IC data standards.	
Common	43. Establish guidance that defines the minimum data protection requirements and progressive levels of data protection reflecting data sensitivity.	• IC CIO & IC CDO w/ DNI/PDDNI Approval and Sensitive Review Group (SRG) Review
Maturing	44. Expand data tagging attributes to support fine-grained access and sharing of sensitive data.	• IC elements



Improve Identity, Credential, and Access Management

Strategic Outcome
Each IC element's access control decisions (person and non-person) align with new ICAM guidance to promulgate IC-wide assured information sharing.
FISMA Activity
▪ Subordinate plans for information security

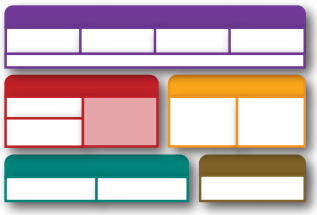
The IC is aligning to the Federal Identity, Credential, and Access Management Framework. IC ICAM services are a fundamental enabler toward strengthening the cybersecurity posture for assured information sharing and better intelligence integration. IC ICAM services will address challenging, multi-network and multi-national requirements and promote consistency of access control and centralized management of key components, such as standards and digital policy.

The IC ICAM reference architecture calls for automated controls to enforce an asset's rights, regardless of the location; more robust digital policy management to allow data stewards to easily define and manage digital policies for assets; and access control based on the environmental-context, such as role, location, and time of day. Robust authentication is critical to these ICAM services, which enable an application to restrict access by verifying that a user's credentials (e.g., public key infrastructure certificate) and user attributes (e.g., clearance, role, organization, country[ies] of affiliation) match the user's data or system privileges.

Managing privileged users is an area of increasing focus. These users require additional verification (e.g., multi-factor authentication using one-time passwords) for more sensitive and secure operations, such as security audit reviews. Authentication enhancements provide additional assurance of a user's role and access to assets managed and controlled by an application. Individuals requiring these additional measures of validation include system administrators and managers who may be able to view the personally identifiable information of others.

Improving Identity, Credential, and Access Management

	Tasks	Champion
Fundamental	45. Limit connections and access to only known person and non-person entities. [3]	• IC elements
	46. Verify that information resources meet minimum ICAM requirements including attribute checks of a person entity's clearance and citizenship or a non-person entity's highest approved classification level and country of affiliation.	
Common	47. Establish minimum criteria for both general and privileged users (PU) [e.g., multi-factor authentication (MFA), "just in time" privileges, and personnel security standards]. [8] [9]	• IC CIO • NCSC
	48. Refactor Federated Identity, Credential, and Access Management policies and standards for the IC.	• IC CIO
Maturing	49. Assess viability of a trust access model to limit potential attack surface across all IC networks (e.g., Trusted Internet Connections, and known gateways, boundaries, and CDSs).	• IC CIO • IC elements



Improve Sharing and Analysis of User Activity Monitoring & Audit Data

Strategic Outcome

Each IC element monitors and shares audit data (person and non-person) internally and with relevant enterprise stakeholders to detect and neutralize nefarious activity as soon as discovered.

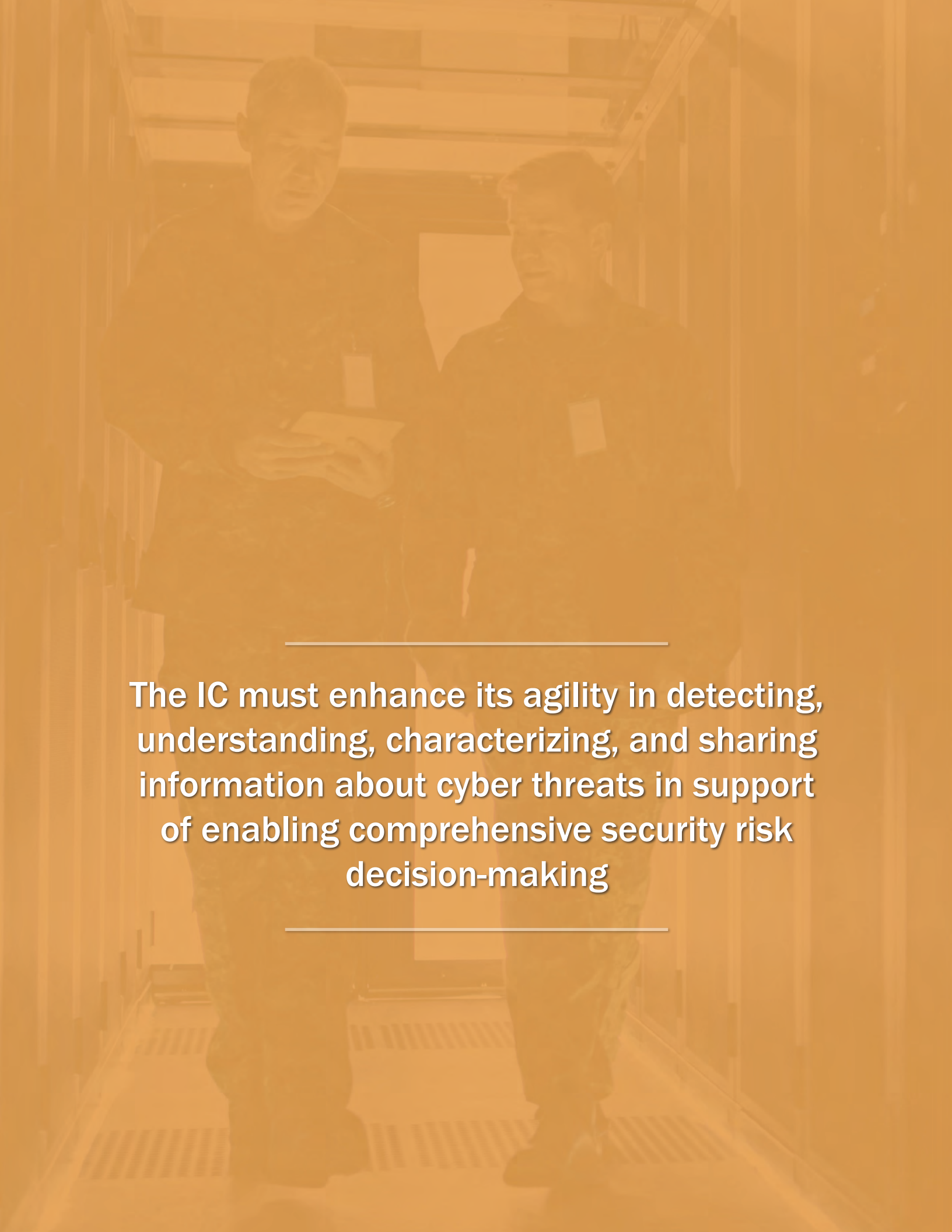
FISMA Activity

- Periodic assessments of the risk
- Subordinate plans for information security

Voluminous audit event generation presents the challenge of discerning user actions of interest from approved activity and system-generated events. The IC continues to improve our ability to detect abusive user activity due to significant efforts towards deploying event capturing agents, implementing collection infrastructure, and integration analysis platforms. Improvements in filtering the generated audit noise to only those events-of-interest, developing rules-based event triggers, sharing triggers among monitoring and detection programs, and integrating behavioral analysis capabilities continue to be areas requiring further investment. Increasing collaboration between enterprise audit, computer network defense (CND), insider threat programs, personnel security, counterintelligence (CI), and privacy through appropriate forums will assist in addressing truly malicious intent or simply accidental disclosures by people or systems.

Improving Sharing and Analysis of User Activity Monitoring and Audit Data

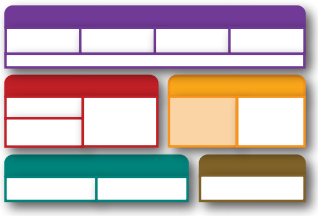
	Tasks	Champion
Fundamental	50. Implement user activity monitoring (UAM) across all types of user/system interactions (i.e., local on device or via proxy) and automate where practical.	• IC elements
	51. Share user attributable audit data with CI, CND, and IT security stakeholders for analysis, respectful of non-US and non-IC partner sharing requirements.	
Common	52. Establish exchange standards for raw audit collection data (e.g., Syslog) complementary to existing IC audit exchange standards.	• IC CIO
	53. Establish guidance for sharing information about high-risk personnel (i.e., contractor and government) and former employees.	• NCSC
	54. Establish procurement mechanism for audit data analytical capabilities and tools.	• IC CIO • ODNI/AP&F
	55. Identify near-real time audit and unauthorized disclosures analysis tools and best practices in collaboration with CI/CND/IT security stakeholders and industry.	
Maturing	56. Identify and establish managed audit enterprise services for enterprise use.	• IC CIO
	57. Explore the potential for IC element and/or IC common data lakes for enterprise audit and UAM data sharing and analysis.	
	58. Monitor environment assisted by behavior-based analysis.	• IC SCC



The IC must enhance its agility in detecting, understanding, characterizing, and sharing information about cyber threats in support of enabling comprehensive security risk decision-making

THREAT INTELLIGENCE SHARING

- Improve Attention to the Supply Chain
- Improve Availability of Threat Intelligence



Improve Attention to the Supply Chain

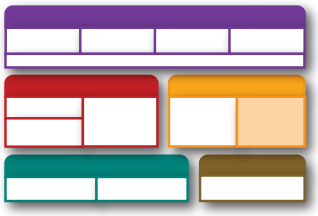
Strategic Outcome
IC functional experts (e.g., CI, CND, and supply chain risk management) seamlessly share near-real time threat intelligence to collaboratively manage risk.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic assessment of the risk and magnitude of harm

Supply chains upon which the U.S. relies, constitute a target rich environment. Their multi-tiered and global nature obfuscate the security, resilience, quality, and delivery of products and technical services. Poor manufacturing and development practices also introduce risks. Adversaries continue to enhance their cyber capabilities and are prolific in attempts to compromise our supply chain using attacks that are inventive, aggressive, sophisticated, and hard to detect. We must raise awareness about vulnerabilities of, threats to, and the need to protect our critical supply chains.

Managing supply chain risk requires frequent communication across complex functional lines of business, many of which do not routinely interact (e.g., acquisition, intelligence, CI, security, human resources, etc.) and governmental bodies (e.g., whole of government, defense, IC, the DIB, and private sector).

Improving Attention to the Supply Chain

	Tasks	Champion
Fundamental	59. Identify and assess suppliers and third-party partners of information systems, components, software, and services using a supply chain risk management (SCRM) process in accordance with ICD 731, *Supply Chain Risk Management*.	• IC elements
	60. Incorporate SCRM findings into acquisition and management decision-making processes across the full life cycle of hardware, software, and services.	
	61. Implement software assurance across software development delivery (i.e., development, test, and operations).	
	62. For acquisition items receiving a threat assessment rating of HIGH or CRITICAL, conduct vulnerability-related testing and analysis to ascertain whether the product has undocumented functionality.	
Common	63. Establish a shared catalog of IC element commercial products risk acceptance decisions.	• NCSC
	64. Establish consistent SCRM methods and training for acquisition and management decisions based upon IC SCRM policy and best practices.	
	65. Identify and procure commercially available data sources, data sharing repository, and analytical tools.	
	66. Establish and mature SCRM governance. [10]	
Maturing	67. Develop a process to provide SCRM Threat Assessment information with the CND and acquisition communities.	• NCSC
	68. Investigate extending supply chain methods and directives to contractor facilities and systems where government data is stored. [1]	
	69. Extend supply chain methods and directives (e.g. ICD 731); including contractors' involvement in asset management life cycle of government property to ensure SCRM requirements are met. [1]	• NCSC • IC elements
	70. Mature processes for electronic waste management, sanitization, and disposal to include investigating services of common concern & extension to contractor systems and facilities.	• IC elements



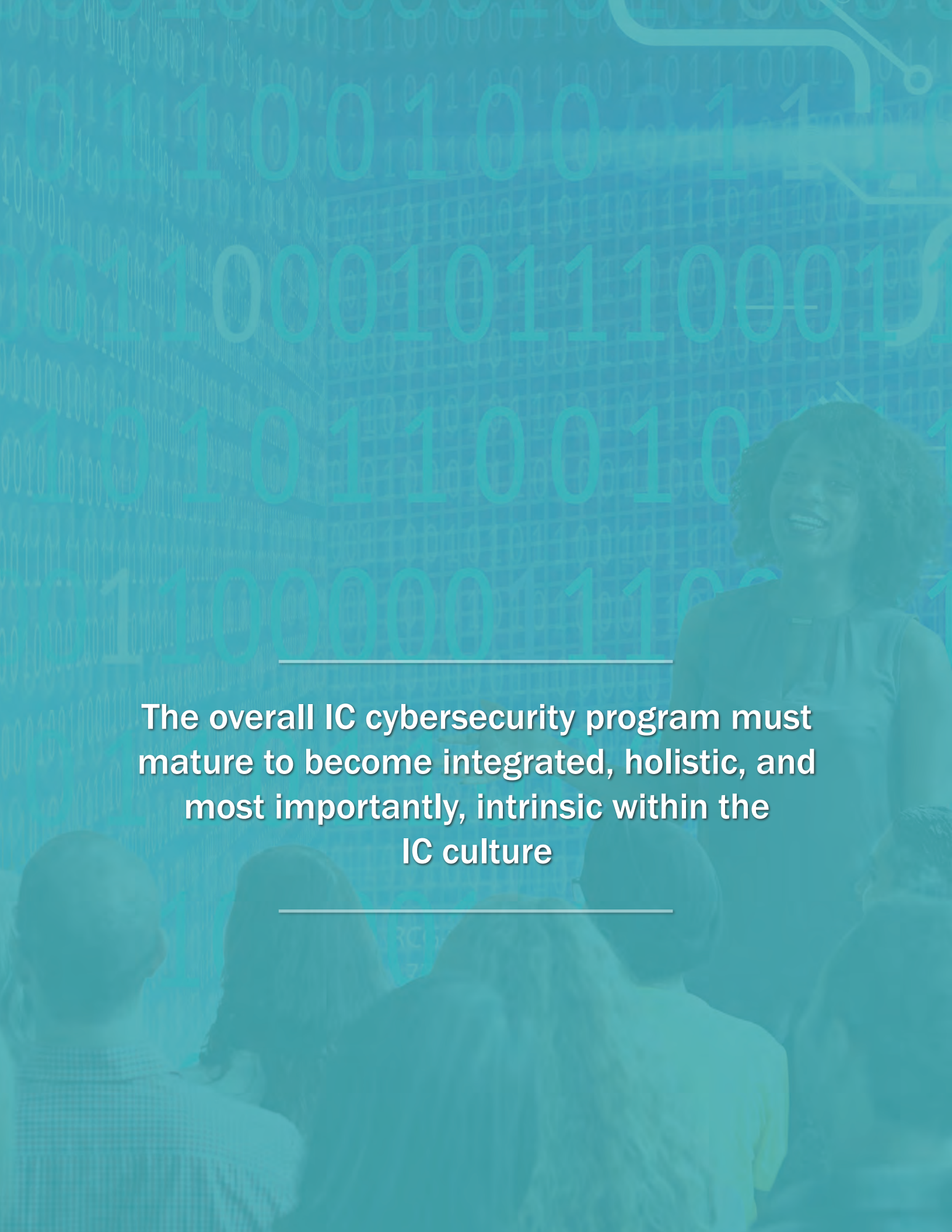
Improve Availability of Threat Intelligence

Strategic Outcome
Each IC element monitors and shares supply chain related risks based on threat intelligence with CI, IT security, and acquisition managers.
FISMA Activity
▪ Subordinate plans for information security

CI and counterterrorism elements must share cyber threat information with IC element supply chain, CND, and enterprise risk functions, as well as the IC SCC, to ensure those operating the IC's networks and systems can effectively identify and efficiently manage security risks. IC elements must likewise recognize their role in a secure, connected, data-centric, integrated, and transparent cybersecurity environment where cybersecurity intelligence is exposed and shared for the benefit to the enterprise. IC elements must resolve long-standing barriers to successful implementation of a shared, secured information environment in which all elements participate and pro-actively protect for the benefit of integrated intelligence mission operations.

Improving Availability of Threat Intelligence

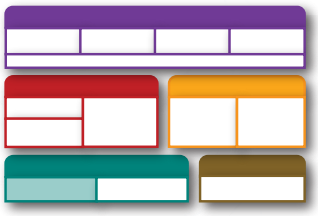
	Tasks	Champion
Fundamental	71. Increase sharing of intelligence cyber threat analyses among CI, CND, and IT security stakeholders (e.g., fully participate in I-Coast). [1]	• IC elements
	72. Relate threat reporting to actual IT vulnerabilities within the network, identify kill chains for each incident, and share to all Computer Incident Response Teams.	
	73. Pursue and improve bi-directional sharing and collaboration relationships with private sector cybersecurity, IT , and telecommunications companies with significant Cyber Threat Intelligence (CTI) insight to broaden awareness of foreign cyber threat activity. [1]	
Common	74. Identify commercial CTI offerings of value and negotiate the purchase and sharing of these services as a single U.S. government enterprise. [2]	• CIA • NSA • FBI
	75. Systematically compile and share CTI lessons learned from significant cyber incidents when they occur. [2]	• CTIIC
	76. Establish a catalog of IC CTI repositories that enables cybersecurity professionals to access the full spectrum of cyber threat intelligence, tailorable to each's distinct set of needs.	• ODNI/NIM-Cyber
Maturing	77. Share threat actor tactics, techniques, and practices related to known vulnerabilities.	• CTIIC • NCSC • ODNI/NIM-Cyber
	78. Assess, test, and implement new organizational and technological mechanisms to better blend regional, technical, and functional analysis of cyber threat activity (e.g., matrixed teams, physical or virtual mission centers, communities of interest, etc.).	• IC elements



The overall IC cybersecurity program must mature to become integrated, holistic, and most importantly, intrinsic within the IC culture

CYBER CAPACITY

- Strengthen Cyber Workforce
- Improve Cyber Programmatic Oversight



Strengthen Cyber Workforce

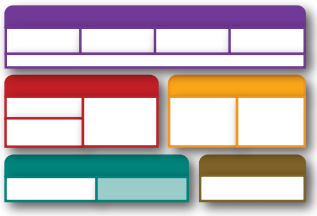
Strategic Outcome
A fully trained and security-aware cyber workforce.
FISMA Activity
▪ Periodic assessments of the risk ▪ Subordinate plans for information security

Developing and maintaining a robust federal cyber workforce sufficiently knowledgeable of cybersecurity topics, issues, and requirements is a challenge. No cybersecurity program is successful without understanding the overarching roles people play in safeguarding our information systems. The IC cyber workforce plays an integral role in maintaining and improving the IC's cybersecurity posture. Cybersecurity professionals are responsible for designing and building secure networks and information systems; identifying and addressing vulnerabilities within those networks and information systems; and collecting and analyzing data to effectively respond to daily threats. Program management, acquisition, and software/systems development processes need to address security up front and remain integrated throughout the entire life cycle.

Strengthening the IC's cybersecurity workforce requires intense and consistent training that keeps cybersecurity professionals up-to-speed in the latest tactics, techniques, and procedures used by adversaries against U.S. information systems. The IC must offer rewarding, unique, and dynamic career opportunities and provide flexibility for professionals in private industry and academia to join the federal service at different times in their careers.

Strengthening the Cyber Workforce

	Tasks	Champion
Fundamental	79. Identify individuals who are accountable and responsible (e.g., functional managers, PMs, systems administrators, information systems security officers, engineers, and managers; CISOs, CIOs, directors, vendors, and contractors) for ensuring cybersecurity is addressed in all enterprise, business, and mission systems and software.	• IC elements
	80. Design long-term cybersecurity workforce staffing and talent development plans reflective of changes in cloud and service architectures, transition to enterprise service use, and increased availability of cyber automation capabilities.	
	81. Develop a cybersecurity workforce retention program, including well-defined career paths, cross training among the larger cyber workforce, and leveraging best practices for performance management, talent development, compensation, and incentive flexibility.	
	82. Create a network of cyber professionals to facilitate knowledge-sharing, development of best practices, cross-discipline exposure, and promotion of a cybersecurity-aware IC element.	
Common	83. Promote IC cyber professional development through cyber competitions, certifications, and credentialing tied to financial and recognition incentives.	• IC elements
	84. Develop an IC cybersecurity orientation program for new cybersecurity professionals.	
	85. Develop and promote cybersecurity career paths, rotational assignments, and mentoring and coaching programs.	



Improve Cyber Programmatic Oversight

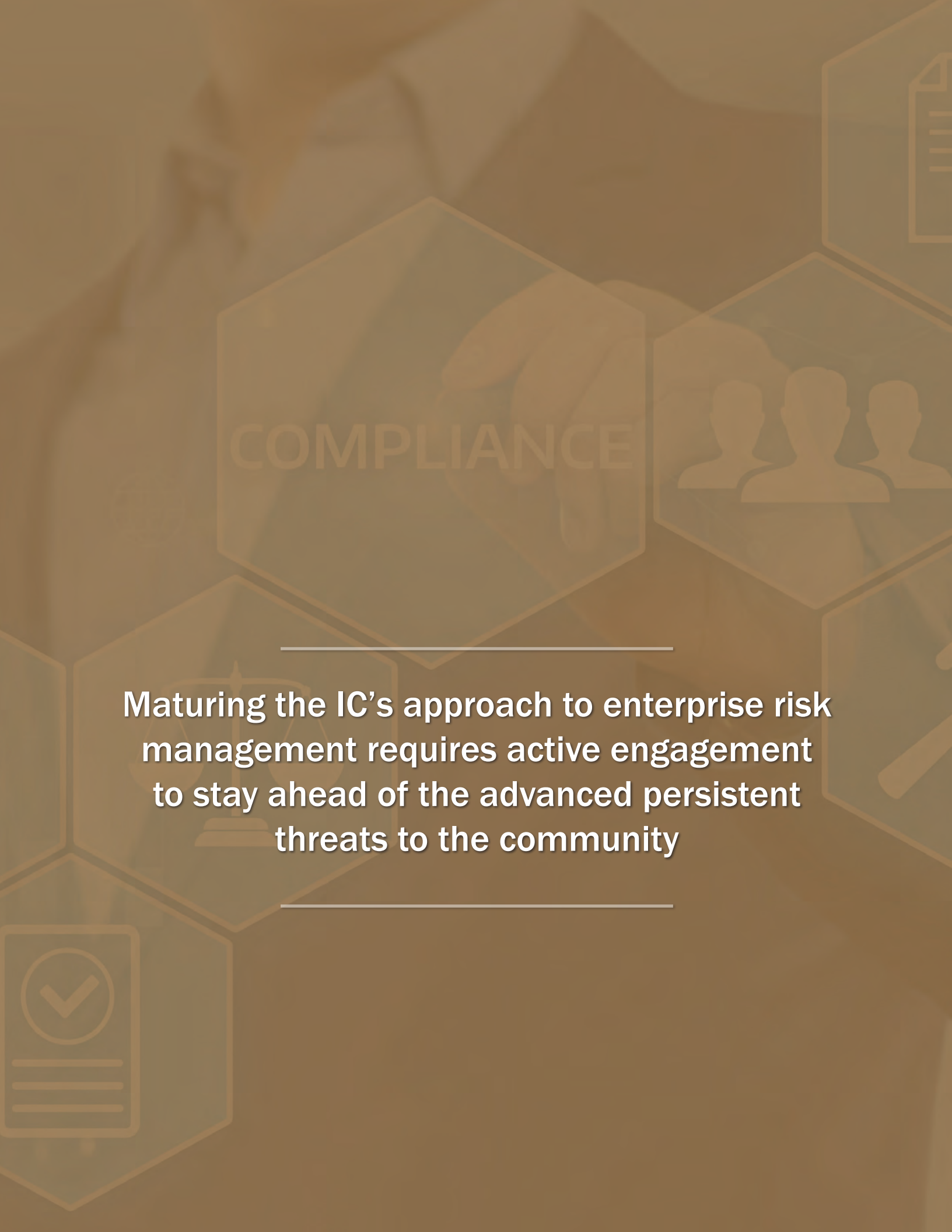
Strategic Outcome
Each IC element implements a Total Asset Management program to identify and manage all of its baseline IT (assets and connectivity) and data.
FISMA Activity
▪ Subordinate plans for information security ▪ Periodic testing and evaluation of effectiveness

The IC is challenged to comprehensively understand the state of the IC IE's cybersecurity posture. FISMA metrics and the *Integrated Defense of the IC IE Annual Report* continually shows little improvement over time. To address this challenge, the IC CIO is developing new reporting and analytic mechanisms, such as the IC IE CPEM, to provide IC leadership a clearer view of the state of progress and to inform decisions regarding priorities, investments, and risks.

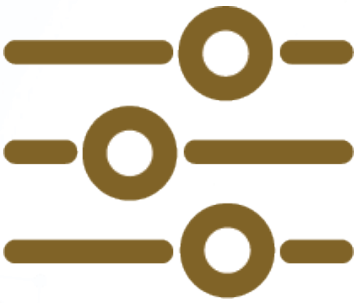
IC elements must continually budget for cybersecurity activities. Some IC elements allocate a significant percentage of their overall operating budget for cybersecurity; however, the resulting reporting does not reflect those investments. IC elements should account for cybersecurity activities in their annual budget builds in response to CIG programmatic requirements and as part of implementing normal cybersecurity best practices.

Improving Cyber Programmatic Oversight

	Tasks	Champion
Fundamental	86. Routinely report key cyber measures identified in the IC IE Cybersecurity Performance Evaluation Model (CPEM) to ODNI. [1]	• IC elements
Common	87. Align and resource information security, and Information and Communications Technology (ICT) supply chain risk management requirements through the Integrated Planning Program Budget and Execution (IPPBE) process.	• IC CIO • NCSC
	88. Establish separate funding codes for cybersecurity.	• IC CFO
Maturing	89. Level-set National Intelligence Program-funded investments across all 17 IC elements for cyber proportionate to each IC element's portfolio and identified gaps.	• IC CFO • IC elements

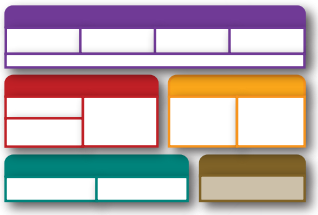


Maturing the IC's approach to enterprise risk management requires active engagement to stay ahead of the advanced persistent threats to the community



CYBER CONTROLS

- Improve Enterprise Risk Management Processes



Improve Enterprise Risk Management Processes

Strategic Outcome
Each IC element employs an agile risk management program throughout acquisition and IT lifecycles to ensure risk management is intrinsic.
FISMA Activity
▪ Periodic assessments of the risk ▪ Policies and procedures ▪ Periodic testing and evaluation of effectiveness

The IC IE is a shared risk environment where decisions made by one IC element affects others. IC elements face fundamental cultural challenges in sharing their respective authorities and responsibilities associated with delivering enterprise, business, and mission IT. Transparency is paramount in sharing information about threats, vulnerabilities, risks, decisions to accept risks, and mitigations.

Increased IC enterprise and service level assessments are needed to bring IC elements together in identifying vulnerabilities. Integrating Service Provider-led joint security assessments with Joint Blue Team penetration testing creates a robust risk-managed capability that identifies those vulnerabilities. These vulnerabilities can then be assessed to determine enterprise risk.

Improving Enterprise Risk Management Processes

	Tasks	Champion
Fundamental	90. Establish streamlined authorization processes that incentivize the use of good security practices and automation.	• IC elements
	91. Leverage existing mission assurance factors (e.g., threat impact severity, exploitability, and IC element exposure) into the prioritization of vulnerability mitigation and mission capability delivery.	
	92. Improve continuous risk management by leveraging asset threat monitoring tools and available threat assessments.	
Common	93. Increase Blue and Red Team testing across IC IE (e.g., data exfiltration attack vectors).	• IC CIO
	94. Identify and track threat actor tactics, techniques, and practices related to known vulnerabilities and prioritize mitigations with IC SCC, CISOs, Authorizing Officials, and others as appropriate.	
	95. Tailor the NIST Cyber Security Framework into an IC Cybersecurity Framework to address IC-unique requirements, to include establishing maturity levels, common vulnerability scoring, minimum risk thresholds, measures, common risk scoring calculus, and benchmarks.	
	96. Establish an executive level IC IE Cybersecurity Performance Evaluation Model (CPEM) scorecard that identifies key performance indicators of the IC's progress to achieve an acceptable cybersecurity posture. [1]	
Maturing	97. Perform ongoing trend analysis of key cyber measures and reflect on the executive level IC IE CPEM.	• IC elements
	98. Implement IC Cybersecurity Framework.	

APPENDICES

- Appendix A – Task Sources
- Appendix B – Index of Tasks by Champion
- Appendix C – Acronyms and Abbreviations

APPENDIX A
TASK SOURCES

[1] *Consolidated Intelligence Guidance for FY2021-2025*, 2019.

[2] *Consolidated Intelligence Guidance for FY2020-2024*, 2018.

[3] IC CIO Memorandum 2017-267, *Effective Vulnerability Management and Routine Information Technology Hygiene*, 13 October 2017.

[4] *FY2017 CIO Federal Information Security Modernization Act (FISMA) Reporting Metrics, Version 1.0*, 2016.

[5] Intelligence Community Standard 502-01, *Intelligence Community Standard 502-01, Intelligence Community Computer Incident Response and Computer Network Defense*, 23 December 2013.

[6] IC CIO Memorandum 2016-0072, *Continuity of Operations Requirements for Intelligence Community Information Technology Enterprise (IC ITE) Service Providers,* 01 September 2016.

[7] Intelligence Community Directive 118, *Intelligence Community Continuity Program (Technical Amendment)*, 20 September 2016.

[8] *NSA Top Ten, NSA Top Ten Cybersecurity Mitigation Strategies*.

[9] ODNI ES 2017-00823, *Office of the Director of National Intelligence 150-Day Report for Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 17 October 2017.

[10] *Consolidated Intelligence Guidance for FY2019-2023*, 2017.

[11] Intelligence Community Directive 502, *Integrated Defense of the Intelligence Community Information Environment*, 11 March 2011.

APPENDIX B
INDEX OF TASKS BY CHAMPION

Champion	Task Identifier
CIA	74
CTIIC	39, 75, 77
FBI	74
IC CDO	43
IC CFO	88, 89
IC CIO	7, 8, 14, 15, 16, 23, 43, 47, 48, 49, 52, 54, 55, 56, 57, 87, 93, 94, 95, 96
IC Elements	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14 (opt), 15 (opt), 17, 18, 19, 20 21, 22, 24, 25, 26, 27, 28, 29, 30, 31, 36, 40, 41, 42, 44, 45, 46, 49, 50, 51, 59, 60, 61, 62, 69, 70, 71, 72, 73, 78, 79, 80, 81, 82, 83, 84, 85, 86, 89, 90, 91, 92, 97, 98
IC SCC	14, 15, 34, 35, 38, 58
NCSC	47, 53, 63, 64, 65, 66, 67, 68, 69, 77, 87
NSA	74
ODNI/AP&F	7, 16, 33
ODNI/NIM-Cyber	32, 37, 76, 77

APPENDIX C
ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AI	Artificial Intelligence
AP&F	Acquisition, Procurement and Facilities
ARF	Asset Reporting Format
ASR	Asset Summary Reporting
CBJB	Congressional Budget Justification Book
CDO	Chief Data Officer
CDS	Cross Domain Solution
CI	Counterintelligence
CIA	Central Intelligence Agency
CIG	Consolidated Intelligence Guidance
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CND	Computer Network Defense
COOP	Continuity of Operations
CPEM	Cybersecurity Performance Evaluation Model
CTI	Cyber Threat Intelligence
CTIIC	Cyber Threat Intelligence Integration Center
CWAA	Cybersecurity Workforce Assessment Act of 2015
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DR	Disaster Recovery
ELA	Enterprise License Agreement

APPENDIX C
ACRONYMS AND ABBREVIATIONS

FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HVA	High Value Asset
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IC CDO	Intelligence Community Chief Data Officer
IC CFO	Intelligence Community Chief Financial Officer
IC CHCO	Intelligence Community Chief Human Capital Office
IC CIO	Intelligence Community Chief Information Officer
ICD	Intelligence Community Directive
IC IE	Intelligence Community Information Environment
ICS	Intelligence Community Standard
IC SCC	Intelligence Community Security Coordination Center
ICT	Information and Communications Technology
IG	Inspector General
IPPBE	Intelligence Planning, Programming, Budgeting, and Evaluation
IR	Incident Response
IT	Information Technology
MCF	Mission Critical Function
MEF	Mission Essential Function
MFA	Multi-Factor Authentication
MIS	Major Issues Study
NCSC	National Counterintelligence and Security Center

APPENDIX C
ACRONYMS AND ABBREVIATIONS

NICE	National Intiative for Cybersecurity Education
NIM	National Intelligence Manager
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
PDDNI	Principal Deputy Director of National Intelligence
PKI	Public Key Infrastructure
PM	Program Manager
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SPB	Strategic Program Briefings
SRG	Senior Review Group
STIG	Security Technical Implementation Guide
UAM	User Activity Monitoring
VM	Vulnerability Management


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA