MITRE | Center for Technology and National Security

INTELLIGENCE AFTER NEXT

THE FUTURE OF THE IC WORKPLACE

by Kent Linnebur, Christine Callsen, Margaret Stromecki, Charles Hedrick

 # 20-2891 10-22-2020

Executive Summary

The Intelligence Community (IC) is at a strategic decision point. The reality of the massive disruption from COVID-19 and the potential for future pandemics compel immediate action to break down entrenched IC barriers to working outside of dedicated classified workplaces.

Various pre-COVID-19 publications have forwarded suggestions for considering some degree of telework in the IC. Herein we dive deeper, providing a holistic view of the IC's interoperability challenges and a roadmap for success. Two major benefits from this shift are **achieving 21ST century operational resiliency** and **growing and sustaining the trusted workforce**.

With COVID-19 changing the calculus for continuity of operations, the IC must evolve to operate a secure infrastructure outside of sensitive compartmented information facilities (SCIFs). With the proper mechanisms in place, many job functions can be done in an unclassified environment. The need for operational resiliency mandates the IC pursue a flexible workplace, recruitment, and retention model across its entire workforce to ensure mission continuity and staff health.

To be successful, the IC must:

- Update policy guidance to establish standard behaviors and expectations across agencies
- Identify work that can be done from home to lower population density in secure facilities
- Identify jobs suitable for the unclassified environment and pilot their implementation
- Establish procedures for new hires to work on unclassified tasks during the security accreditation process
- Increase critical-skills pay and offer a flexible work environment to recruit, promote and retain high-value talent

COVID-19 WILL NOT BE A ONE-OFF EVENT, AND THE UNEXPECTED WILL CONTINUALLY CHALLENGE THE CURRENT SCIF-ONLY WORK ENVIRONMENT

- Include advisory and commercial contractors as part of the trusted workforce

Evolution of the IC to achieve these benefits aligns along three pillars, with a discrete set of actions necessary for success:

- **Establishing Policy Solutions for the Digital Age**
  - Update information environment policies.
  - Improve cross domain solutions for discovery and collaboration across security enclaves, protecting information against inadvertent disclosure, especially classified and personally identifiable information.
  - Provide reciprocity for security adjudication and for IT applications.
  - Promote interoperability and sharing across the enterprise.
- **Embracing Tradecraft in the Open Source World**
  - Strategically develop and share data sources and tradecraft to improve global security.
  - Move large subsets of open source intelligence to unclassified networks for ease of access.
  - Operate in the public domain, within coalitions of nations to counter the influences of malicious actors.
  - Perform suitable activities transparently in public, in coordination with partner nations, non-governmental organizations, industry, and academia.

- **Implementing a Trusted and Secure Network Infrastructure**
  - Support employee awareness, address architecture strength and weakness, incorporate enterprise risk management, minimize enterprise vulnerabilities, and enable time-critical cyber situational awareness.
  - Expand use of the unclassified cloud, leveraging zero-trust architecture, coupled with security protocols, to create a defense-in-depth approach to protecting information.
  - Evaluate commercially available collaboration tools to facilitate such an environment.

An added benefit to the IC and the workforce is the inherent cost savings provided by leveraging work outside the SCIF. Reductions in the population inside the SCIF significantly reduces facility costs (i.e., demand for expanded or new facilities). Allowing staff to work from home eliminates commute time and stress and allows for increased productivity. Moving unclassified data to integrated unclassified infrastructure will also yield savings and minimize duplication across the networks.

The failure to aggressively pursue a more robust, resilient, and flexible workplace environment will result in a serious degradation in the viability of the IC. By affording a new generation of intelligence professionals with the most capable tools, resources and workplace options, the IC will be able to compete for the best talent available.

Introduction

The push to a flexible model balancing traditional SCIF work with telework and open source analysis is critical to the future of the IC workplace. COVID-19 will not be a one-off event; there will be other challenges to our current SCIF-only work environment. Progress will only be achieved when IC leadership embraces a change from the entrenched culture of insulation and provides the community with the guidance, practices, and tools to complete the mission from any location.

This consideration is hardly new. Past studies have recommended models that allow the IC to work from unclassified spaces. A 2018 RAND study, for example, suggested a shift based on an examination of "how various federal agencies enable employees to work with sensitive information outside government facilities [2]." Published two years before the current pandemic, the report discussed potential benefits, including expanded collaboration across external partners and continuity in the event of a natural disaster. But the study considered telework by government employees only. And until now, no one could fathom—and thus shape recommendations for—a disruption to the work environment of COVID-19 proportions.

Lack of movement toward this model reflects a century's worth of entrenched identity: windowless rooms, conversations contained within four walls, outdated processes, and—above all—resistance to change. The reality of long-term, massive disruption from COVID-19 and potential future pandemics compels immediate action to break down these cultural barriers. At a minimum, employees need increased flexibility to accommodate childcare and healthcare concerns during such crises. Lowering population density in classified workspaces also will be critical in the future.

The IC must rethink intelligence with the specific goal of consciously shifting appropriate elements to the unclassified domain.

We envision two major benefits from this shift toward increasing work outside the SCIF:

- Achieving 21ST century operational resiliency
- Growing and sustaining the trusted workforce

21st Century Operational Resiliency

Operational resilience encompasses the planning and convergence of activities to ensure that an enterprise and the environment it operates in are able to identify and mitigate risks that can lead to disruptions (man-made, natural, accidental or intentional) and recover and restore mission critical operations within acceptable timelines [3]. In the modern era of integrated operations, the IC must evolve beyond the current approaches for continuity of operations (COOP). IC resiliency in the 21st century mandates operating in a highly connected virtual world where information is gleaned from both classified and unclassified sources and analysis can leverage a more robust and diverse selection of all-source data products.

Operating solely within the confines of the closed networks and SCIFs currently employed by the IC inhibits collaboration across the military, industrial, and academic communities where much needed resources reside. The Joint All-Domain Command and Control (JADC2) system is an evolution of the way the Department of Defense (DoD) will operate in the "everything is connected" world. The IC also must evolve by creating a more flexible and resilient IC operating model to significantly expand the ability to collect, analyze, disseminate, and receive raw and finished intelligence in a variety of other crisis environments. It will extend the reach across US government facilities around the world and improve the timeliness of intelligence support to policymakers and warfighters alike.

Although COVID-19 may be referred to as a "once-in-a-100-year event," we cannot count on avoiding a similar event for another century. The IC must leverage technology that affords operations using a secure infrastructure outside a SCIF. The pandemic has given leadership insight into the constraints imposed by the current environment of primarily working within SCIFs.

A more flexible and survivable IC enterprise integrated with collateral and unclassified networks to mitigate the risk of future disruptions is essential to resilient operations in the future.

Growing and Sustaining the Trusted Workforce

The COVID-19 crisis is a proving ground for flexible work solutions. Millions of Americans are now taking advantage of these arrangements. The need for operational resiliency mandates the IC pursue flexibility wherever possible, without delay, to ensure mission continuity, the health of its workforce, and its ability to attract and retain the strongest and most capable workforce.

The nonpartisan, nonprofit Intelligence and National Security Alliance (INSA) has called for reforms to support IC workforce development efforts, including more agile and responsive processes to attract the next generation workforce. INSA's recommendations center around mission focus, competitive pay structures, career growth flexibility across the IC and between the government and private sector and making the security clearance process more efficient [4]. New initiatives across the IC have started to recognize the benefits of incorporating more flexible working conditions to foster recruitment of the next generation workforce.
We fully support the INSA recommendations and the new initiatives. The following recommendations are provided to continue the process for growing and sustaining a trusted workforce.

- **Standardize behavior and expectations.** Agencies need to develop clear policy guidance (e.g., location, reporting, oversight) governing telework and incorporate this into existing and future contracts. This will minimize misinterpretation of requirements.

- **Identify work that can be done from home in the event of national crises or individual requirements like health issues.** At a virtual Town Hall in May 2020, the Director of the National Reconnaissance Office (NRO) announced the mandate that all NRO supervisors develop unclassified projects for each employee, comprising 20 percent of their work schedule. This will fulfill the mission while lowering density in secure facilities—a model for other agencies.
- **Identify types of work that can be accomplished in an unclassified environment** (e.g., human resources, finance, research) and pilot those jobs as telework opportunities. As pilots mature, agencies will have a cadre of full or part-time teleworkers to ensure operational resiliency. Additionally, designated telework positions would boost recruitment and allow agencies to draw expertise from a larger and more diverse geographic pool.
- **Improve on-boarding by allowing new hires to work probationally on unclassified tasking** or training during the security accreditation process. The contractor workforce employs this model, and the government should implement similar processes.
- **Increase critical-skills pay and offer a flexible work environment to incentivize and attract high-value talent.** The IC is losing or failing to attract highly skilled workers who have opportunities to do similar work for commercial companies with less restrictive work environments and higher compensation and benefits. To remain competitive, the IC needs to offer a more flexible work model with more competitive pay.
- **Extend the IC's trusted workforce beyond government employees to comprise a fully vetted, trusted, agile workforce.** The IC must leverage, embrace, and incentivize its entire team of civilian, military, federally funded research and development center, and contractor personnel to work efficiently together to protect national security. Opportunities to bring together a more diverse and robust cadre in open venues to solve IC mission challenges is essential to the viability of the IC.

THE IC MUST RE-THINK INTELLIGENCE WITH THE SPECIFIC GOAL OF CONSCIOUSLY SHIFTING APPROPRIATE ELEMENTS TO THE UNCLASSIFIED DOMAIN.

Ultimately the IC will need to address the broader security, personnel, and resource issues surrounding telework and the nature of secure environments. As the government grapples with COVID-19-related constraints for the near future, agencies need to address the co-mingling of classified and unclassified materials on classified systems. To maximize workforce contributions, agencies should extract unclassified information, move it to the appropriate unclassified systems, and shift the workload to those same systems.

Momentum is building in this direction, as evidenced by the 2019 Director of National Intelligence (DNI) "Right, Trusted, Agile Workforce" strategic workforce development initiative [5]. Telework, flexible schedules, virtual collaboration, and cutting-edge technology solutions will deliver a competitive advantage for those working in defense of the nation. The cost benefits for the move to remote work are also significant, both to the government and the workforce. Studies have shown that:

- On average, hourly earnings in the top 15 metro areas are over 40% higher for the same occupation in the rest of the U.S. [6]

- Costs per square foot for a SCIF vary but are roughly double the costs for standard office space. With the percentage of staff able to work remotely increasing from 16% to 49%, occupancy in SCIFs has reduced the overcrowding and the demand for more space.
- Working from home saves the staff roughly $2000 per year and reduces the number of cars on the road, resulting in less traffic, congestion, and pollution.
- Remote work will spread productivity to other geographically dispersed talent pools (essentially fueling the creation of the largest labor market in the world). [6]

Establishing Policy Solutions for the Digital Age

The IC Information Environment (IE) Data Strategy [7] provides a framework for evolving tradecraft and policies for information management. The community is already considering using open source and big data analytics to forecast adversary trends. The IC must evolve its policies to meet the demands for operations in the 21st century. Our recommendations include:

- **Update policy for managing the IC IE,** following guidance from IC Directive 121 [8], which mandates the move toward cloud computing and Services of Common Concern. The need to enable endpoint protections, regardless of network classification, fits within this directive. This includes multi-factor authentication (MFA) and at-rest and in-transit data encryption.
- **Provide better cross domain solutions for discovery and collaboration** across security enclaves to minimize redundant storage across infrastructure. Policy updates are needed to mature and accredit more robust cross domain solutions; remote management processes for attached devices; and identity/access management controls.
- **Reform the processing and sharing of security clearance and accreditation information between the members of the IC.** The executive order [9] for transferring clearance vetting from the Office of Personnel Management to the DoD is a positive step. The IC should provide reciprocity for security adjudication and for SCIF and non-SCIF action.
- **Provide reciprocity for IT applications hosted on the network.** Allow for accelerated adoption of tools and resources. If vetted by one agency, applications should be reciprocally available to the rest of the IC.
- **Revise policies to mandate interoperability and sharing across the enterprise.** Each IC agency endeavors to protect its resources and justify its impact for national security. Collaborative development of policies and procedures are required to ensure that each agency's contribution is recognized. IC leadership must incentivize the workforce to participate in opportunities for joint engagements and product development.

Embracing Tradecraft in the Open-Source World

Former DNI Daniel Coats stated, "Our nation faces an ever-evolving, increasingly complex, and diverse set of threats. The IC is charged with the responsibility of providing the most timely, accurate, and insightful intelligence to counter these threats. Rapid advances in technology have led to an explosion in the volume, velocity, and variety of data, and we must find innovative ways to exploit and establish relevance and ensure the veracity of our information [7]."

Exploitable information resides beyond the IC's protected network infrastructure. Open Source Intelligence (OSINT) is providing a much-needed boost to IC tradecraft. Particularly with the advent of data science applied against large data sets, unclassified exploitation has been producing valuable and actionable information.

The U.S. is not alone in recognizing the importance of OSINT. Malicious actors seek to exploit public resources and steal intellectual property for their own interests and to the detriment of citizens globally. To build coalitions of nations to counter these influences, the IC must operate in the public domain, exposing these actors in the same spaces where they exert influence.

Intelligence activities like cyber defense and socio-cultural mapping must be done transparently in public in coordination with partner nations, non-govern-mental organizations, industry, and academia. The IC should develop and share data sources and tradecraft in these areas to improve global security. We cannot rely on industry to defeat malicious actors. We must support research in artificial intelligence and machine learning to support exploitation of the large volumes of information and identify efforts that promulgate false information.

Ultimately, large subsets of geospatial intelligence and OSINT should be moved wholesale to unclassified networks, with smaller cadres of analysts in classified spaces to fuse this unclassified intelligence with classified data sources.

Implementing a Trusted and Secure Network Infrastructure

The IC has previously recognized the need to better leverage the open internet and provide tools to merge information safely and securely across security domains. Specialized procedures and capabilities limited to a few approved users are currently required to transmit data between networks of varying classification levels.

The primary risk for IC operations outside the SCIF is inadvertent disclosure of information to unauthorized entities—a risk that could bring significant cost and impact.

Therefore, any concepts for working outside the SCIF must incorporate a trusted and verifiable enterprise network configuration control and management environment. Essential components of this environment must:

- **Support employee awareness.** Mandate user training on access, use, and cybersecurity responsibilities for all remote access and collaboration capabilities
- **Address architecture strength and weakness.** Configure, monitor, and manage remote access and collaboration capabilities using public and private cloud service-provided virtual desktop services
- **Mature cybersecurity.** Improve remote network management and integrity verification and deploy automated methods to detect attempts at unauthorized intrusions
- **Realize enterprise risk management.** Implement procedures to mitigate risks to network, information, and personnel against potential threats
- **Minimize enterprise vulnerabilities.** Provide automated patch installation for software collaboration products hosted on government-provided servers
- **Enable time-critical cyber situational awareness.** Incorporate measures to assess the network and automatically respond to anomalous behaviors or activity patterns

IT Security: What Does the Future of Cloud Look Like for the IC?

The consolidation of the IT infrastructure using cloud computing and storage has enabled the IC to improve collaboration and sharing across the enterprise. The IC employs the cloud in both classified and unclassified networks. Each agency has developed their approach for cloud instantiations using unique internal guidelines

and procedures. Under COVID-19, the rate of adoption for the unclassified cloud environment is increasing [10], allowing for a greater balance between work in secure and unclassified environments.

To improve collaboration across IC and DoD network operations in the cloud, leadership must pursue a more standardized approach for interoperability across cloud implementations. Administration, though initially cumbersome, will mature as organizations adopt this capability. In principle and practice, the IC will leverage zero-trust architecture techniques and platforms, and virtual and session-based environments, coupled with a host of access controls and security protocols, to create a defense-in-depth approach to protecting its intellectual capital and crown jewels.

The inherent architecture and orchestration of cloud services will compel federal agencies to go beyond antiquated means of protection. Because the cloud is built on software defined networks (SDN), enhanced security practices within the system boundary are increasing in demand. Cloud service providers like Amazon Web Services and Microsoft Azure offer their own built-in security capabilities, and the IC (generally) has enterprise services that can be leveraged together with these environments to strengthen its overall security posture.

The IC needs to set the "rules of the road" to ensure smart, efficient, and transferable adoption of the unclassified cloud across agencies, even if they must do some tailoring to meet their individual needs. The IC must increase transparency and communication and follow common standards so that we achieve true interoperability in this highly connected enterprise.

Collaboration Tools

Numerous commercially available collaboration tools can support a broadly distributed workforce. Organizations may also develop tools for their unique mission. The various capabilities offered in collaboration tools include email, text chat, file sharing, videoconferencing, white boarding, and task management, among others. No single application suite currently provides a solution for all collaboration needs. Many of the tools allow for integration with other tools to approach a complete solution. The security of these tools can be an issue, depending upon where the data is stored, how it is shared, and how it is transmitted. As a result, the IC would benefit from an independent application integration organization to provide reference solutions to the community. This organization would ensure these tools meet community standards for functionality and interoperability. Certification of the applications should be accepted by each member of the community. Each member should also have inputs to the accreditation process to accelerate adoption on their networks.

Conclusion

The push to a flexible, hybrid model combining traditional work in SCIFs with remote operations and open source information analysis is critical to the future of the IC workplace, and to the future capabilities of the IC. Progress will only be achieved when the IC embraces a change from an entrenched culture of insulation to a more flexible work environment. COVID-19 will not be a one-off event, and the unexpected will continually challenge the current SCIF-only work environment. This effort also will provide fiscal savings for all segments of the IC with reduced demand for expensive facilities and increased geographic diversity in the workforce. We now have the opportunity, impetus, and a clearly realized incentive to redefine IC workplace norms.

The move toward a robust, secure multi-location work environment across the IC will require time to prototype, test, and validate to prevent both inadvertent and intentional data breaches. Rapid growth and maturity in collaboration tools will be required to provide the necessary capabilities for this distributed workforce.

Across the community, agencies are establishing policies to move outside the SCIF, but they are doing this internally. It is imperative that the IC come together and establish community-wide policies and procedures for flexible remote operations.

As Bill Evanina, Director of the National Counterintelligence and Security Center, stated in a recent INSA webinar, "Just because you have a top-secret clearance doesn't mean you can't work at home to do a percentage of your job. ... As we move aggressively toward what that might look like, we have to find effective solutions to protect that work, protect that employee and protect our communications from the adversaries, who are actually actively watching how we do this right now [11]."

References

[1] C. Clancy, "COVID-19 is forcing the intelligence community to think outside the SCIF," April 2020. [Online]. Available: https://thehill.com/opinion/national-security/490983-covid-19-is-forcing-the-intelligence-community-to-think-outside-the

[2] RAND, "Moving to the Unclassified," The RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2024.html

[3] N. Mehravari, "ABCs of Ops Resilience", Software Engineering Institute, March 2013, [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=293887

[4] C. Alsup, N. Morra, "Making Intelligence Careers Appealing to Millennials, Intelligence and National Security Alliance," [Online]. Available: https://news.clearancejobs.com/2018/04/02/making-intelligence-careers-appealing-millennials/

[5] Office of the Director of National Intelligence, "Transformation & Innovation - What We Do" [Online]. Available: https://www.odni.gov/index.php/who-we-are/organizations/strategy-engagement/ti/ti-what-we-do

[6] B. Booth, "Pandemic job shift: A lot more work is about to head outside America's highest-priced cities", {Online] Available: https://www.cnbc.com/2020/07/23/pandemic-job-shift-more-work-headed-outside-high-priced-us-cities.html

[7] Office of the Director of National Intelligence, "Intelligence Community Information Environment Data Strategy 2017-2021," [Online]. Available: https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf

[8] Office of the Director of National Intelligence, "Intelligence Community Directive 121 - Managing the Intelligence Community Information Environment," January 2017. [Online]. Available: https://www.dni.gov/files/documents/ICD/ICD%20121%20-%20Managing%20the%20IC%20Information%20Environment%20(19%20Jan%202017).pdf

[9] Office of the President, "Executive Order Executive Order on Transferring Responsibility for Background Investigations to the Department of Defense," [Online]. Available: https://www.whitehouse.gov/presidential-actions/executive-order-transferring-responsibility-background-investigations-department-defense/

[10] R. Magoulas, S. Swoyer, O'Reilly Survey: Cloud Adoption in 2020. May 2020. [Online]. Available: https://www.oreilly.com/radar/cloud-adoption-in-2020/

[11] B. Evanina in N. Ogrysko, "Could the pandemic force the intelligence community to reconsider workplace flexibilities?," May 2020. [Online]. Available: https://federalnewsnetwork.com/workforce/2020/05/could-the-pandemic-force-the-intelligence-community-to-reconsider-workplace-flexibilities/

Authors

Kent Linnebur is an Outcome Leader at MITRE and has spent over 40 years working in DOD and IC programs with specific focus in MASINT and ELINT collection systems. He currently works on space surveillance modeling and simulation. He holds a BS in Engineering Science from the University of Cincinnati.

Christine Callsen is currently leading the Futures Office at MITRE Labs. She previously spent over a decade working in academia, most recently serving as the Managing Director for the Hume Center for National Security and Technology at Virginia Tech. She holds BS and MS degrees from the University of Wisconsin.

Margaret Stromecki is a Principal Business Strategist at MITRE with expertise in governance, strategic planning, and organizational change. She transitioned to her current role following an 18-year career at CIA as an analyst, manager, and senior executive. Margaret has a BA from Cornell and a master's degree from Columbia University.

Charles Hedrick is a GEOINT Project Leader in MITRE's Space Department where he performs strategic planning and information assurance. He's supported various agencies across the IC. He holds a CISSP with a BS in Integrated Science and Technology (ISAT) from James Madison and an MS in Cyber Security from Maryland.

Intelligence After Next

MITRE strives to stimulate thought, dialogue and action for national security leaders developing the plans, policy and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities and concerns of the Intelligence Community's analytical workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat or to detail the integrated solutions and enabling technologies needed to ensure the success of the IC's analytical community in the post-COVID-19 world.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | Center for Technology & National Security