NATIONAL SECURITY SPACE ASSOCIATION

Establish Governance and Align Security Policies and Programs to Enable U.S. National Security Space Missions

Studies & Analysis Center,

National Security Space Association

October 29, 2020

Endorsed By

INSA

USGIF
United States Geospatial Intelligence Foundation

Contractor SAP Security Working Group

Establish Governance and Align Security Policies and Programs

to Enable U.S. National Security Space Missions

Executive Summary

The United States is engaged in a great power competition and confronting an increasing array of threats from state and non-state actors. The imperative to deter the threat or use of force in space, acquire advanced capabilities that outpace the threat and sustain U.S. comparative advantages in space, and plan and execute space operations to deter or if necessary prevail in a conflict involving space, provides an unprecedented opportunity for the federal government to work together and with the private sector in novel ways to address security challenges and opportunities. To this end, the National Security Space Association recommends that serious attention be given to the following recommendations regarding how to establish security governance and align security policies and programs to enable U.S. national security space missions.

1. **Establish interagency security governance to enable execution of national security space missions.** The Secretary of Defense and Director of National Intelligence should establish a senior level interagency security board with membership from the DoD components and IC agencies with space-related research, development, and acquisition programs and operational activities to provide comprehensive security governance of the national security space program and partner, as appropriate, with other space agencies.

2. **Modify DoD security governance to incorporate the new space management structure**. The Defense Security Enterprise (DSE), and DSE Executive Committee (ExCom), that provide direction for a comprehensive DSE policy and oversight framework and governance to safeguard personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences, should be modified to incorporate the executive leadership of the national security space enterprise.

3. **Review and update security policies, centralize policy formulation and oversight, and decentralize security services execution.** DoD and IC space-related policies should be reviewed and updated to address today's international security environment, adopt a risk management framework, and enable acquisition speed and operational agility.

4. **Promulgate overarching security classification policy that enables proper classification and consistent program execution.** The Assistant Secretary of Defense for Space Policy should review, coordinate, and promulgate policy guidance regarding classification of DoD space programs and activities to enable consistent, efficient, and effective program execution and oversight as well as provide the basis for configuration management enforcing consistency among multiple organizations and programs.

5. **Reestablish layered security architectures to enhance program protection.** The national security space program should reestablish a security architecture approach that includes multiple layers of access categories to protect classified information, while enabling, as appropriate and necessary,

coordination, collaboration, and sharing of intelligence, technical, and operational information within the U.S. government, across U.S. space sectors, and with allies and partners.

6. **Establish reciprocity for accesses and security between the DoD and IC.** Reciprocity should be established among the DoD Components and IC agencies for DoD, National Intelligence Program- and Military Intelligence Program-funded space programs. Legislation or executive-level agreements between the DoD and the IC should be put in place to facilitate the joint-use and co-use of facilities, SCI personnel accesses, secure networks, communications, and clearance adjudication decisions.

7. **Realign and empower program office security services**. A layered protection strategy and plan for new national security space programs should be included in the acquisition strategy reviewed by the Space Acquisition Council and approved by the Acquisition Executive with the authority to proceed. Program Executive Officers and their direct reports then should be accountable for the security performance of their programs. In turn, Program Security Officers should be placed under Program Director's management to align incentives for security and compliance with program cost, schedule, and performance.

8. **Establish partnerships between the U.S. Space Force, U.S. Space Command, and other security organizations.** The leadership of the USSF and USSPACECOM should establish top-down relationships and partner with their counterparts at both DCSA and DIA to ensure mission-responsive security support for personnel vetting, collateral and SCI facilities/networks, intelligence and counterintelligence, national interest determination approvals, and industry oversight.

9. **Consider establishing an executive-level security position for the Defense space program.** This position could report to the USSF's Chief of Space Operations or the Assistant Secretary of the Air Force for Space Acquisition and Integration to administer the interagency executive board, coordinate with other DoD and IC security and intelligence organizations, and oversee implementation of approved changes to security procedures and practices.

10. **Include properly trained and compensated security professionals as part of the dedicated national security space acquisition workforce.** Managing and executing development and procurement programs that deliver capability uncompromised must be a part of the space acquisition workforce's education and training. Consequently, security should be included as a sub-specialty as a new space acquisition force is being established by the USSF.

11. **Create deeper government-industry partnerships**. The U.S. government should adjust security to enable industry contractors to align their technologies, capabilities, planning, and investment with the USSF. Key contractor teams should be given the necessary insight into the DoD's Unclassified to SAP architectures to enable informed contractor-funded IRAD, the creation of innovative solutions to capability gaps, and the opportunity to create, adapt, evolve, and integrate their products aligned to the USSF mission.

12. **Prioritize digital transformation and convergence of classified IT networks.** The USSF should prioritize digital transformation and become a fast-follower where possible to enable classified digital design and manufacturing, multi-classification modeling and simulation solutions, and more efficient and secure classified IT networks. In addition, U.S. government and industry secure information technology networks should be converged to eliminate waste, increase agility, and address cyber threats.

13. **Facilitate robust modeling, simulation, analytics, and wargaming across all classification levels.** Physics-based simulation, advanced computational modeling, and other automated analytic tools and techniques are necessary to support rigorous systems engineering and architecture analyses as well as wargaming in support of critical government decision-making processes.

Establish Governance and Align Security Policies and Programs to Enable U.S. National Security Space Missions

Introduction

The United States is engaged in a great power competition and confronts an increasing array of threats from state and non-state actors. China and Russia seek to reshape the world in ways favorable to their interests by undermining the rules-based international order at the expense of the security and well-being of the United States, our allies, and partners. While China is a rising power and Russia is a declining power, both are dangerous. China recently moved on Hong Kong, had a border skirmish with India, conducted military operations near Taiwan, and continues to construct and fortify military installations in the South China Sea. Russia has moved abruptly into Crimea, Ukraine, Syria, and Libya. These actions reflect Xi's and Putin's mindsets and propensity for risk-taking.

Beijing's and Moscow's national security strategies make clear they intend to inhibit the United States ability to deter or respond to aggression by degrading or defeating U.S. intelligence gathering and decision-making processes as well as information and communications technology (ICT) networks and systems. China and Russia are aggressively conducting espionage activities and modernizing their armed forces. Their foreign intelligence services conduct human and technical intelligence-gathering in conjunction with economic espionage, supply chain operations, and computer network exploitation to penetrate critical infrastructure, information networks, and facilities in order to steal commercial, sensitive, and classified information, technology, and intellectual property. Beijing and Moscow are developing, testing, and deploying an array of sophisticated new military capabilities, including nuclear, hypersonic, cyber, space, and counterspace systems for anti-access/area-denial, and conducting "grey zone" operations below the classic threshold of armed attack.

Importantly, China and Russia are moving aggressively to undermine U.S. strategic advantages in space. They understand the value of space assets to the United States and the advantage we gain by integrating capabilities in all domains. U.S. space capabilities and vulnerabilities remain a collection priority of Beijing's and Moscow's espionage activities. This information informs their design and operation of space and counterspace systems (as highlighted by their recent anti-satellite weapons tests and deployments), to threaten freedom of access and use of space, jeopardize U.S. and allied military forces, and place the United States at risk.

In response, the U.S. government has promulgated new space policies and strategies, including direction to enhance Department of Defense (DoD) and Intelligence Community (IC) space collaboration, establish the U.S. Space Force (USSF), reestablish U.S. Space Command (USSPACECOM), and strengthen multinational Operation Olympic Defender. The U.S. government has not yet systematically addressed security governance or services, however, as part of the response. Current and former senior U.S. officials have observed that security is often an impediment rather than an enabler of national security space missions. The critique includes, among other things: over-classification of programs; too many stove-piped classified network; overextended industrial-age security services that do not keep pace and adversely impact program cost and schedule; obstacles to sharing intelligence, technical, and operational information across the U.S. space sectors as well as with allies and partners; barriers to establishing credible deterrence and reassurance against space threats; and obstructions to planning, modeling and simulation, training, exercising, and conducting joint, interagency, and combined space operations.

The imperative to deter the threat or use of force in space, acquire advanced capabilities that outpace the threat and sustain U.S. comparative advantages in space, and plan and execute space operations to deter or if necessary prevail in a conflict involving space, provides an unprecedented opportunity for the federal government to work together and with the private sector in novel ways to address security challenges and opportunities. To this end, the National Security Space Association recommends that serious attention be given to the following analysis and recommendations for establishing security governance and align security services to enable U.S. national security space missions.

Background

The U.S. national security space program was initiated in the early stages of the Cold War. A catalyst was the imperative to prevent strategic surprise given the advent of atomic and thermonuclear weapons, long-range bombers, and ballistic missiles. Confronted by the unprecedented Soviet nuclear threat to the nation's survival, the U.S. government and industry created the means to overfly the Iron Curtain and access hostile and denied territory to pierce the veil of secrecy shrouding the USSR's leadership intentions and military capabilities, offset the Red Army's conventional superiority in Europe, and contain Soviet power and influence in Eurasia.

Security organizations, policy guidance, and practices established to protect U.S. national security and foreign relations have evolved since the end of World War II. The implementation of security measures are governed by different entities, various statutes, directives, executive orders, and regulations such as: the National Security Act of 1947, as amended; Executive Order 13526, "Classified National Security Information"; DoD Directive 5205.07, "Special Access Program Policy"; Intelligence Community Directive 703, "Protection of Classified National Intelligence, including Sensitive Compartmented Information"; and DoD Manual 5220.22-M, "National Industrial Security Program Operations Manual". Every defense and intelligence space program must follow such rules. The rules provide best practices for the U.S. government and industry contractors to safeguard information, technologies, personnel, and operations. With few exceptions, the rules may be waived if impractical or unreasonable to comply with. The process for doing so, however, is arduous, time consuming, and requires the intervention and approval of senior government officials.

Cold War

The U.S. national security space program, and associated security practices, were driven by the exigencies of the Soviet-American nuclear confrontation. The policy framework established to safeguard national space security missions implemented Presidential direction for classifying, safeguarding, and declassifying information. Information was classified Confidential, Secret, or Top Secret if its unauthorized disclosure could reasonably be expected to cause damage, serious damage, or grave damage, respectively, to national security.

The national security space program was purposely classified at multiple levels to limit need-to-know and protect sensitive information. It evolved from a specialized research and development culture that was highly compartmentalized across acquisition and operations. A layered approach to program protection was standard practice to protect essential national security information while permitting both government and industry to share information and collaborate to carry out space missions, functions, and tasks. Personnel, physical, information, industrial, and operations security measures

were implemented as a bulwark against threats to the national security space workforce, technology, information, and missions.

Moreover, special security measures were undertaken to safeguard U.S. technological and operational advantages. Sensitive Compartmented Information (SCI), i.e., intelligence information concerning or derived from intelligence sources, methods, or analytical processes, was protected by formal access control systems. Special Access Programs (SAPs) were established when collateral classification measures were insufficient and absolutely necessary to protect the most sensitive capabilities, information, technologies, and operations. To implement SCI and SAP controls, special security officers, special security representatives, and contractor special security representatives were established to ensure personnel, information, and industrial security as well as operate secure facilities. SAP, or so-called "black" programs, which might also contain SCI, used need-to-know and access controls beyond those normally provided for access to Collateral or Confidential, Secret, and Top Secret information. When a program is designated as a SAP, need-to-know is centrally controlled and the government maintains strict accountability for who is accessed and what facilities and information processing systems are approved.

Access to SAPs in the U.S. government and industry was very tightly controlled and oversight was streamlined in both the executive and legislative branches. Members of Congress assigned to designated defense and intelligence committees were authorized access to SAPs within the respective committee's SAP oversight role, except for exceptionally sensitive or "waived" programs. Unless approved by the Secretary of Defense, only the chair, the ranking minority member, and the staff directors of the defense and intelligence committees were authorized access to waived SAPs within their committee's respective SAP oversight role.

Post-Cold War

The U.S. altered its security posture after the Cold War ended. With the dissolution of the USSR and the Warsaw Pact, the threat was expected to diminish. Substantial amounts of classified information were downgraded or declassified. Operations security practices were modified regarding space launches and other information about national security space missions. Moreover, requirements for space system protection and survivability were traded-off for improved performance and cost savings given the expectation that space was a benign domain that would remain a sanctuary from conflict.

The United States demonstrated the technological and operational advantages produced by the aerospace and defense industry in the 1991 Persian Gulf war. While America achieved a swift victory, the need to address burdensome security issues to improve operations and intelligence coordination and deconfliction was one of the U.S. lessons learned from the conflict. Meanwhile, adversaries learned that the timely integration of space capabilities for warfighting was essential to U.S. military-technological prowess and battlespace dominance. Consequently, Beijing and Moscow intensified their espionage activities, illicit military and technology acquisition, indigenous weapons systems procurements, and other efforts to better understand U.S. weaknesses and counter our capabilities.

By the turn of the century, foreign knowledge of U.S. defense and intelligence space capabilities had significantly increased through space object surveillance and identification, international cooperation, espionage, media disclosures, and U.S. diplomatic demarches. Indeed, espionage cases

both during and after the Cold War, such as Glenn Souther, William Kampiles, Aldrich Ames, and Robert Hanssen, among others, gravely damaged U.S. national security. Personnel security practices to address the "insider threat" were reevaluated and strengthened following damage assessments. Likewise, physical security practices were enhanced following the 9/11 terrorist attacks.

In 2001, both the National Security Space Management and Organization Commission and the NRO Commission recommended that the U.S. government increase the use of compartmentation to enhance the protection of critical defense and intelligence space programs. That recommendation was prescient in light of the subsequent extensive unauthorized disclosure of classified information by Edward Snowden in 2013 as well as penetration and large scale computer network exploitation of U.S. government and industrial base ICT networks by China and Russia. Information and operations security must continue to evolve in response to the advanced persistent cyber threat as well as the growth of international and commercial remote sensing space capabilities.

Today

The U.S. is now competing against nation-state powers with sophisticated intelligence-gathering and weapons systems. In particular, fast-paced counterspace, including cyber, threats to space assets are turning inside the U.S. government's acquisition cycle. There is general recognition that the U.S. military technological lead is eroding, significant capability increases are needed every 3-5 years to address the threat cycles, and current acquisition models are not conducive to capitalizing on the frequent evolution of information, communications, and other advanced technology, largely driven by the private sector. While the federal government has begun restructuring national security space management and organization to accelerate the acquisition, fielding, and operation of modern and resilient space capabilities, it has not yet addressed the complex and decentralized security enterprise supporting the space mission.

Security governance and services that support the national security space program involve numerous DoD components and IC agencies. These include: the Office of the Under Secretary of Defense for Intelligence; DoD SAP Central Office; multiple Department of Air Force organizations such as the Special Security Office, field Special Security Offices, SAP Central Office, and Air Force Office of Special Investigation; National Counterintelligence and Security Center; NRO; Defense Intelligence Agency (DIA); Defense Counterintelligence and Security Agency (DCSA); and individual acquisition program office and operational unit security personnel. Under the National Industrial Security Program overseen by DCSA, contractor security organizations provide security services for more than 10,000 cleared companies. These organizations interface with the federal government regarding accesses, accreditation of facilities, information systems, and networks, and visitor controls, as well as administer and provide other services.

Security services are an essential and pacing function for all classified (Collateral, SCI, and SAP) national security space programs. At a minimum, classified programs require a cleared workforce, accredited facilities, and accredited secure IT systems and networks. Indeed, all three are prerequisites for both the government and industry to achieve mission success. Programs, including government program offices, operational units, and industry contractors cannot operate more efficiently or effectively than they are enabled by supporting security services.

Although the 2018 Director of National Intelligence's Security Executive Agency Directive 7, "Reciprocity of Background Investigations and National Security Adjudications," mandates reciprocity across the federal government, many execution-level security organizations are not compliant with this policy. Similarly, while DoD has a single authoritative personnel security database for SAPs that contains individual eligibility information, reciprocity is not consistently applied, and some security personnel do not use the information in the database. Program Security Questionnaires and other eligibility documentation are frequently requested consuming valuable government and industry man-hours and delaying workforce vetting. In the aggregate, this has a significant detrimental effect on the government and industry national security space workforce productivity.

The mix of outdated, evolving, and new security policies, classification guidance, security architectures, and security organizations are producing inconsistencies in the application of security measures. Indeed, unintended consequences from differing interpretations and application of policy and guidance impose costs and risks as well as hinder mission performance. They are creating unnecessary challenges to the efficient and effective conduct of the national security space program.

These challenges include providing effective governance and configuration management; creating comprehensive and layered security architectures; enabling proper accesses, coordination, and information sharing within and among DoD components as well as between the DoD, IC, and other federal departments and agencies; and enabling information sharing between the U.S. government and private sector as well as with allies and partners. These challenges impede:

- Improving space threat intelligence and threat awareness;
- Establishing credible deterrence and reassurance;
- Developing modeling, simulation, and analytic tools for space acquisition and portfolio management decision support;
- Collaborating for efficient research, technology development, engineering, test, and evaluation of new capabilities;
- Avoiding unnecessary stove-piping and duplication of effort among research, development, and production programs;
- Acquiring space capabilities with agility at the speed of relevance;
- Integrating space capabilities into operations and contingency plans;
- Conducting training and exercises involving multiple levels of classification; and
- Planning and executing joint, interagency, and combined space operations.

Moreover, industry is in an untenable position dealing with various U.S. government security organizations' inconsistencies, particularly regarding classification, accesses, and accreditation, given the threat of reduced award fees, loss of clearances, decertification, and other sanctions. Security infractions or violations have been alleged by one government agency for unauthorized disclosure of information previously put in the public domain or formally authorized to be disclosed by another within the same executive department. Similarly, security infractions or violations have been alleged by one government agency disregarding the level of classification of information by another agency that collected it and was the Original Classification Authority (OCA). Independent research and development efforts funded by industry have been precluded that would be of considerable benefit to multiple government agencies. Joint-use and co-use of facilities, secure networks, and communications

commonly have been disapproved requiring travel and other expenses to perform work in an approved facility across the country.

Smaller companies, new entrants, and purely commercial companies often are precluded from competing for government business because they cannot obtain accesses or accreditation of facilities to know of or respond to classified requests for proposals. The burden of the actual and opportunity costs to industry of such unintended consequences and, by extension the mission, are substantial. A company may have an unclassified product, for example, that is used on numerous classified programs with classified data. The cleared contractor support personnel have great difficulty maintaining their clearances or cleared workspace because the rules demand that a classified contract be put in place when a classified contract is not required. Accredited facilities currently cannot be shared across SAP and SCI programs. As a result, the U.S. government is denying itself access to new ideas, technology, capabilities, and applications.

Consequently, it is imperative to establish governance and align security policies and programs to enable, rather than impede, U.S. national security space missions. Governance must ensure proper and consistently applied classification and security services must provide appropriate safeguards while supporting acquisition speed, operational agility, and mission effectiveness. Risks and tensions among security, information sharing, speed, and agility must be managed more effectively. The national security space enterprise must be secure, avoid past mistakes, and leverage opportunities to comprehend and counter the threat in order to sustain U.S. advantages in space.

Recommendations

The need to outpace and counter the rapidly evolving threat is an urgent matter that requires bipartisan support, informed decisions, and bold actions in both the public and private sectors. While the U.S. government has restructured national security space management and organization, begun reforming acquisition processes, and initiated efforts to enhance collaboration with the other U.S. space sectors, allies, and partners, it has not reevaluated how to govern and deliver security services to enable national security space missions. Security is complex, decentralized, cumbersome, and inconsistent. Rather than serving to enable mission success, security is creating challenges that impede achieving policy objectives, efficiently managing programs and resources, sharing information internal to the U.S. government as well as with our allies and partners, and preparing warfighters to deter, fight, and win. This point has been echoed by senior Department officials.

Thus, the national security space enterprise must improve the way it governs security, provides security services, and implements security procedures to establish effective deterrence and reassurance, accelerate the development and fielding of new space capabilities, and ensure warfighting readiness. This will involve difficult changes to culture, organizational constructs, and operating models as well as deeper partnership between the U.S. government and industry. The following recommendations summarize the changes necessary to establish governance and align security services to enable U.S. national security space missions.

Establish interagency security governance to enable execution of national security space missions. The Secretary of Defense and Director of National Intelligence should establish a senior level interagency security board with membership from the DoD components and IC agencies with space-related research, development, and acquisition programs and operational activities to provide

comprehensive security governance of the national security space program and partner, as appropriate, with other space agencies. The board would oversee the implementation and enforcement of policy and guidance; foster connected secure information technology; enable information sharing internal to the U.S. government, with the private sector, and with allies and international partners; provide insight into space-related security matters; streamline security processes; drive uniform application of security practices; adjudicate and resolve issues arising from inconsistencies; ensure proper classification and access to perform space missions, functions, and tasks; and enable reciprocity and enhanced DoD and IC space collaboration. It would also provide configuration management and review original classification decisions and program governance annually to support effective oversight. It would also develop a legislative strategy to request any necessary statutory authorities or resources required to align security to enable U.S. national security space missions. Lastly, this board could evaluate policy changes, reciprocity, and other ideas that can increase the efficiency of the government and contractor workforce to reduce the impact of the pandemic on classified operations.

Modify DoD security governance to incorporate the new space management structure. The Defense Security Enterprise (DSE), and DSE Executive Committee (ExCom), that provide direction for a comprehensive DSE policy and oversight framework and governance to safeguard personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences, should be modified to incorporate the executive leadership of the national security space enterprise. In addition, an OSD SAP executive-level space portfolio should be maintained and a space sub-portfolio should be established to align space planning and investment, eliminate unnecessary redundancy among DoD components' programs, and enable integration. Furthermore, either the Department of the Air Force should amend the charter and membership of the Special Programs Oversight Committee (SPOC) or the USSF should establish its own SPOC to enable informed governance, centralize security policy, and oversee decentralized security execution. OSD SAP "super-user" billets should be allocated for key USSF and USSPACECOM leadership to enable awareness of and executive engagement on enterprise-wide matters.

Review and update security policies, centralize policy formulation and oversight, and decentralize security services execution. DoD and IC space-related policies should be reviewed and updated to address today's international security environment, adopt a risk management framework, and enable acquisition speed and operational agility. Security policies can then be tailored consistent with DoD and IC authorities, responsibilities, missions, and roles. Security policies should be coordinated and harmonized through the DSE ExCom and interagency security board to align authority, responsibility, accountability, and resources and instill a culture that fosters risk management. Centralized policy formulation and oversight would enable timely identification and resolution of inconsistencies, while decentralized implementation would continue to ensure responsive delivery of security services across the enterprise.

Promulgate overarching security classification policy that enables proper classification and consistent program execution. The Assistant Secretary of Defense for Space Policy should review, analyze, coordinate, and promulgate policy guidance regarding classification of DoD space programs and activities. Issuance of overarching classification guidance and intent would enable consistent, efficient, and effective program execution and oversight. Moreover, it would provide the basis for configuration management thereby enforcing consistency among multiple organizations and programs. The policy should provide a framework and guidelines for capabilities that would be openly acknowledged to

support pre-war deterrence of adversary aggression, capabilities that would be concealed to provide technological and operational advantages for wartime application, and capabilities that would be held as war reserves and only revealed as necessary for intra-war deterrence, escalation control, or war-winning. It should enable the USSF and USSPACECOM to develop doctrine, operational art, and tactics, techniques and procedures for employing such capabilities. In addition, it should enable ongoing global warfighting integration efforts to facilitate horizontal operations and contingency planning as well as planning for combined multi-domain operations. The policy should enable the USSF and USSPACECOM to gain appropriate insight into all SAPs relevant to their missions as well as leverage the resources, talent, technology, and know-how of the private sector as well as allies and trusted partners. Indeed, it should enable U.S. warfighters to train and exercise how they will fight with such capabilities. Further, the policy should limit the number of space-related Original Classification Authority (OCAs) within DoD and require annual review of space classification decisions to ensure compliance with policy and intent. Indeed, the Department should strictly enforce the requirement for component heads to annually review and validate SAPs to ensure alignment with the security classification policy. In this regard, the USSF should work with the other services and components with OCAs to ensure both consistent classification and awareness of space activities. Where possible, coordination with the IC should occur to attempt to align DoD and IC classification guidance.

Reestablish layered security architectures to enhance program protection. The national security space program should reestablish prior DoD security best practices designed to protect essential national security information, facilitate government and industry collaboration to advance technology development and mission capability, enable effective declaratory policy, and ensure senior leaders and warfighters have access to the information necessary to perform their missions. This security architecture approach resembles an "onion skin" with multiple layers of access categories, from Unclassified to Collateral (Confidential, Secret, and Top Secret) to SCI and SAP (acknowledged, unacknowledged, and waived) to protect classified information, while enabling, as appropriate and necessary, coordination and sharing of intelligence and technical and operational information within the U.S. government, across the U.S. space sectors, and with allies and partners. This approach, with all layers, should be mandatory; any exception should require the approval of the DSE ExCom or interagency security board. The layered security approach also involves the formation of multiple groupings or portfolios to meet security and access needs. Such "umbrella" portfolios can include multiple compartments and sub-compartments distinguished by mission and class or by type and effect. Within compartments, sub-compartments can be created to limit compromise and protect selected operations, acquisitions, and technology developments, including architecture and mission area level analysis. The layered structure will permit government and industry to collaborate across missions, capabilities, and programs while maintaining the integrity of the security architecture. It will allow industry to invest in and execute internal research and development programs by enabling technology to be worked on at different security levels without requiring access to specifics about programs or operational activities. Moreover, it will facilitate sharing of information, analyses, concepts, architectures, and technologies that will help avoid creating duplication or gaps.

Establish reciprocity for accesses and security between the DoD and IC. Reciprocity should be established among the DoD Components and IC agencies for DoD, National Intelligence Program- and Military Intelligence Program-funded space programs. Legislation or executive-level agreements between the DoD and the IC should be put in place to facilitate the joint-use and co-use of facilities, SCI

personnel accesses, secure networks, and communications (this is vital today with travel and other restrictions associated with the recent pandemic). Reciprocity should be mandated regarding the SAP eligibility and adjudication process to eliminate inefficiency and oversight entities should ensure execution-level security organizations comply with and consistently apply standing policy guidance regarding reciprocity. In addition, SAP security architectures with mirror compartments should be created to enable informed oversight by the Office of the Secretary of Defense, Office of the Director of National Intelligence, and Congressional oversight committees. Space programs and operations are uniquely challenged because they require both SAP clearances administered by the DoD and SCI access administered by the Intelligence Community. To preclude adverse impacts to programs and operations, SAP and SCI processes for personnel access, facilities, and IT should be executed concurrently rather than independently and sequentially. Moreover, at USSPACECOM, operations and intelligence staffs with space mission responsibilities should be cross-briefed on relevant SAPs and SCI compartments and sub-compartments.

Realign and empower program office security services. The layered protection strategy and plan for new national security space programs should be included in the acquisition strategy reviewed by the Space Acquisition Council and approved by the Acquisition Executive as part of the formal "authority to proceed" process. Program Executive Officers and their direct reports should be accountable for the security performance of their programs. In turn, Program Security Officers should be placed under Program Director's management to align incentives for security and compliance with program cost, schedule, and performance. Rather than continuing to make decisions about implementation of security policy at high levels and slowing program execution, the government should accelerate execution by delegating decision authority to program offices. Further, security professionals should be incentivized to develop innovative and secure ways to enable programs as well as build in redundancy for critical security services to eliminate single point failures.

Establish partnerships between the USSF, USSPACECOM, and other security organizations. The leadership of the USSF and USSPACECOM should establish top-down relationships and partner with their counterparts at both DCSA and DIA to ensure mission responsive security support for personnel vetting, collateral and SCI facilities/networks, intelligence and counterintelligence, national interest determination approvals, and industry oversight. Representatives from DCSA, DIA, and other intelligence and security organizations should be detailed to the USSF to facilitate collaboration.

Consider establishing an executive-level security position for the Defense space program. This position should report to the USSF's Chief of Space Operations or the Assistant Secretary of the Air Force for Space Acquisition and Integration. Duties may include administering the interagency executive board, coordinating with other DoD and IC security and intelligence organizations, and overseeing approved changes to security procedures and practices. Staff should include detailees from DoD and IC security and intelligence organizations such as DCSA and DIA. This official should also have a hotline to enable government and industry to inform directly the USSF senior security official of any security concern hindering program or mission execution.

Include properly trained and compensated security professionals as part of the dedicated national security space acquisition workforce. Managing and executing development and procurement programs that deliver uncompromised capabilities must be a part of the space acquisition workforce's education and training. Consequently, security should be included as a sub-specialty as a new space

acquisition force is being established by the USSF. Security must be included in the specialized education system and corresponding specialized career development system specifically tailored for the unique acquisition needs of space systems. The curriculum should include the breadth of security disciplines for risk management of classified programs. Career management and compensation for security professionals should be reviewed to ensure the national security space enterprise is attracting, retaining, and developing talent.

Create deeper government-industry partnerships. The U.S. government should adjust security to enable industry contractors to align their technologies, capabilities, planning, and investment with the USSF. Key contractor teams should be given the necessary insight into the DoD's Unclassified to SAP architectures to enable informed contractor-funded IRAD, the creation of innovative solutions to capability gaps, and the opportunity to create, adapt, evolve, and integrate their products aligned to USSF missions. In addition, policies that limit accesses to industry executive leadership and key supporting functional staff should be modified to allow them to perform their fiduciary and oversight responsibilities. This will help to avoid putting companies in a reactive posture and preventing them from being able to bring the necessary talent and resources to bear in support of critical programs. The Under Secretary of Defense for Acquisition and Sustainment and DoD SAPCO have developed and are staffing for approval a Corporate Portfolio Program policy that will provide defense industry access to SAP programs under contract. This policy will enable industry to meet their fiduciary responsibilities and better enable cross-program integration. In addition, a security education exchange program between government and industry should be implemented to improve awareness and understanding of each other's perspectives and security challenges.

Prioritize digital transformation and convergence of classified IT networks. The USSF should prioritize digital transformation and become a fast-follower where possible to enable classified digital design and manufacturing, multi-classification modeling and simulation solutions, and more efficient and secure classified IT network. In addition, U.S. government and industry secure information technology networks should be converged to eliminate waste, increase agility, and address cyber threats. Too many IT networks (e.g., SIPRNET, JWICS, and thousands of SAP networks) in government and industry inhibit the ability to collaborate, share, and move data and information. Indeed, the coronavirus pandemic has highlighted the need for connected secure networks and collaboration tools. It is also difficult to manage and protect all of these networks. The national security space program thus should leverage the following ongoing pathfinding initiatives. First, DARPA's partnership with the DoD CIO and DIA to pilot an initiative to push JWICS to defense industry will help to address the insufficient access to certain classified networks that impedes industry's ability, among other things, to collaborate and monitor threat developments. Industry must be equipped with the necessary tools to stay abreast of the threat. While many defense industrial base companies have SCI accesses and several have existing JWICs accounts (usually accessed from a government site), obtaining JWICs accounts within defense industry SCIFs is extremely difficult. JWICs access should be expanded to properly cleared defense industry contractors. This could be implemented quickly and at low cost by utilizing existing DoD component SAP enterprise networks already deployed to industry. Second, continue the DoD CIO's investment in SAP digital transformation with a cloud architecture and strategy to connect the defense enterprise, enterprise applications, and solutions for large defense industry (Industry Connections or ICON). In conjunction with a layered security architecture, a secure IT system that can operate at the portfolio or sub-compartment level of each user will enable better communication and collaboration between users and greatly simplifies logistical matters such as document access and sharing. An IT system designed around such layered protection eliminates the need to replicate work and technologies

for multiple organizations and missions. Properly implemented, Protection Level 3 and 4 IT systems also will facilitate coordination and collaboration across mission areas, programs, industry, and government while maintaining effective compartmentation. Networks like ICON and enterprise secure VTCs are vital and should be accelerated especially with travel and other restrictions associated with the recent pandemic. Third, move out aggressively to implement proven cross-domain access solutions to provide users with the ability to access multiple independent levels of security on a single workstation, including access to classified networks from unclassified environments. Various cross-domain solutions exist to provide for high-to-low and low-to-high connectivity and utilize NSA-approved (Raise the Bar) commercial solutions for classified programs. The USSF should sponsor demonstrations of government and industry use cases that would increase workforce efficiency and reduce the impacts of the pandemic on classified operations.

Facilitate robust modeling, simulation, analytics, and wargaming across all classification levels. Physics-based simulation, advanced computational modeling, and other automated analytic tools and techniques are necessary to support rigorous systems engineering and architecture analyses as well as wargaming in support of critical government decision-making processes. A security framework should be established to facilitate robust, all domain M&S, analyses, and wargaming for both government and industry to support the national security space program. The DoD Chief Information Officer's "SAP cloud" already in use today should be considered for piloting such a capability.