Functional Bureau Strategy

Bureau of Diplomatic Security

FOR PUBLIC RELEASE

Approved: 05/21/2018

Table of Contents

1. Executive Statement

The Department of State (DOS) is the lead U.S. foreign affairs agency within the Executive Branch and the lead institution for the conduct of U.S. diplomacy. The Bureau of Diplomatic Security (DS), established under the Omnibus Diplomatic Security and Antiterrorism Act of 1986, provides a secure environment for conducting U.S. diplomacy and promoting U.S. interests worldwide. DS is the most widely represented U.S. law enforcement and security agency in the world, protecting people, property, and information at over 270 Department missions around the globe. It is the only such organization that possesses the core capabilities needed to enable a comprehensive law enforcement and security posture in domestic and overseas locations, positioning DS as a leader in security management for the United States and the world.

In the years ahead, DS will confront a future where the challenges facing the world provide unprecedented opportunities for U.S. diplomacy. Yet, the places where diplomatic presence is most needed are often those in which it can be the most dangerous to operate. DS works daily to reduce the risks inherent in diplomatic work, though the risk will never be eliminated entirely. DS also faces a central challenge: at the same time that its mission is expected to become more complex by operating in more dangerous environments, it must balance quickly aligning resources to priorities with an unpredictable federal budget process.

The DS FY 2018-2022 Functional Bureau Strategy (FBS) is a strategic document that aims to guide DS in the years ahead to operate in myriad environments where U.S. diplomacy deems a presence. The FBS is not intended to be an operational document; therefore, it does not focus on enabling day-to-day activities for the Bureau. Rather, it highlights areas where DS must continue to strengthen its capabilities and grow in order to be effectively positioned for the future.

Summary of FY 2018 – FY2022 Strategic Goals

1) Secure U.S. foreign affairs activity in all operating environments, domestically and abroad, to advance U.S. diplomacy.

2) Protect the homeland and the integrity of U.S. travel documents through effective and efficient investigations to prevent harm to the U.S. and its citizens from criminal and terrorist activity.

3) Provide high quality training to equip DOS and U.S. government personnel engaged in U.S. foreign affairs, as well as DOS dependents, with the right skills to safely and successfully operate in the current threat environment.

4) Invest in a skilled, dedicated, trusted, diverse, and inclusive workforce to realize the mission of DS more effectively.

5) Harness the right innovative technologies and business processes to protect the DOS's global infrastructure and information assets, and operate safely in a digital environment.

6) Cross-cutting Management Goal: Demonstrate strong and effective leadership and management of DS to provide the foundation for an agile, proactive, and flexible security organization.

DS Vision Statement

Be an agile, proactive, and flexible security and law enforcement organization to further U.S. diplomacy and meet the security demands of operating in a more complicated and dangerous world.

DS Mission Statement

Provide a safe and secure platform for the conduct of U.S. foreign policy through the protection of life, property, and information.

Methodology and Approach

To inform the FBS, DS deputy assistant secretaries and equivalents, all office directors, and select program managers were interviewed to gather information designed to assist the Bureau in articulating its strategic mission, goals, objectives, and key measures. In addition, DS reviewed and analyzed existing policy and mission requirements to identify where the Bureau should focus in the future. DS reviewed Office of Inspector General (OIG) and Government Accountability Office (GAO) congressional reports, and the Joint Department and USAID FY 2018-2022 Strategic Plan (JSP) to ensure alignment of the FBS with the broader strategy of DOS and U.S. government priorities. The FBS also establishes performance indicators and milestones, which measure progress toward achieving strategic goals, inform future resource allocation, and ensure accountability of all programs and individuals. The FBS will be used as a leadership tool to communicate DS's broader vision, mission, and strategic direction, and to help align program activities to budget requests.

2. Bureau Strategic Framework

Strategy Outline

Bureau Goal 1: Secure U.S. foreign affairs activity in all operating environments, domestically and abroad, to advance U.S. diplomacy.

> **Bureau Objective 1.1:** Enhance, enact, and enforce security standards to protect personnel, property, and information worldwide.
>
> **Bureau Objective 1.2:** Lead in the protective operations field by collecting, publishing, and implementing continuous improvements based on lessons learned, and defining and demonstrating best practices.
>
> **Bureau Objective 1.3**: Leverage intelligence information and timely access to resources to operate safely and effectively, particularly in significant threat areas and critical situations.
>
> **Bureau Objective 1.4:** Protect networks, IT assets, and information from cyber threats.
>
> **Bureau Objective 1.5:** Prevent harm from insider threats by identifying those whose actions intentionally or unintentionally pose risk to the Department and its assets.

Bureau Goal 2: Protect the homeland and the integrity of U.S. travel documents through effective and efficient investigations to prevent harm to the United States and its citizens from criminal and terrorist activity.

> **Bureau Objective 2.1:** Leverage all resources and stakeholders for investigating U.S. passport and visa fraud to successfully refer cases to support Department priorities.
>
> **Bureau Objective 2.2:** Conduct high-quality and efficient investigations that protect the integrity of U.S. travel documents.
>
> **Bureau Objective 2.3:** Support investigations of U.S. travel document fraud by strengthening investigative capacity.

Bureau Goal 3: Provide high-quality training to equip Department and other U.S. government personnel engaged in U.S. foreign affairs, as well as Department dependents, with the right skills to safely and successfully operate in the current threat environment.

Bureau Objective 3.1: Consolidate hard-skills training at the Foreign Affairs Security Training Center (FASTC) to improve training efficiency and achieve cost efficiencies.

Bureau Objective 3.2: Ensure that DS and Department workforce is consistently trained and capable of meeting the challenges posed by the current threat environment.

Bureau Objective 3.3: Provide a management system for training to align resources to priorities for effective human capital planning.

Bureau Goal 4: Invest in a skilled, dedicated, trusted, diverse, and inclusive workforce to realize the mission of DS more effectively.

Bureau Objective 4.1: Cultivate effective leaders and managers who are trained for excellence and get the best results from their staff.

Bureau Objective 4.2: Work together across DS to fill positions and align staff resources to Bureau priorities.

Bureau Objective 4.3: Recruit, develop, and retain a skilled and committed workforce.

Bureau Goal 5: Harness the right technologies and business processes to innovate and safely operate in a digital environment.

Bureau Objective 5.1: Become a digital and data-driven organization by employing the right technology, talent, and processes to operate effectively and accomplish the mission.

Bureau Objective 5.2: Leverage digital tools to quickly distribute safety, threat, and other information, and communicate effectively with the public.

Bureau Objective 5.3: Standardize common platforms and architectures within DS to avoid duplicative IT investments and to allow for an effective IT portfolio management system.

Bureau Objective 5.4: Expand classified systems to protect sensitive, classified, and intelligence information.

Cross-cutting Management Goal 6: Demonstrate strong and effective leadership and management of the Bureau to provide the foundation for an agile, proactive, and flexible security organization.

Cross-cutting Management Objective 6.1: Manage Bureau finances through effective budgeting and resource allocation.

Cross-cutting Management Objective 6.2: Strategically enhance intra-agency relationships to enable DS to quickly leverage the authorities and capabilities of partner agencies in executing its mission.

Cross-cutting Management Objective 6.3: Streamline the procurement process to ensure purchasing requests are met in a timely manner, especially for mission critical needs.

Cross-cutting Management Objective 6.4: Promote critical thinking and problem-solving skills to become a more solutions-driven organization.

Cross-cutting Management Objective 6.5: Pursue organizational excellence through effective program performance management and leadership.

Cross-cutting Management Objective 6.6: Educate and inform DS program stakeholders through effective internal and external communications.

3. Goals and Objectives

Bureau Goal 1: Secure U.S. foreign affairs activity in all operating environments, domestically and abroad, to advance U.S. diplomacy.

a. Description and Linkages

To be effective in the years ahead, DS must proactively assess risks and strengthen its ability to respond. Achieving this goal requires strategies in priority areas - including fulfilling DS's key responsibilities of developing and ensuring compliance with security standards, being a leader in protective security operations, operating efficiently and effectively in high threat areas, and protecting DOS against cyber and insider threats. This goal aligns to Goal 4, Objective 4.4 of the JSP.

b. Key Partners and Stakeholders

Countermeasures (DS/C), Cyber and Technology Security (DS/CTS), Domestic Operations (DS/DO), Executive (DS/EX), High Threat Programs (DS/HTP), International Programs (DS/IP), Security Infrastructure (DS/SI), Training (DS/T) and Threat Investigations and Analysis (DS/TIA).

Bureau Objective 1.1: Enhance, enact, and enforce security standards to protect personnel, property, and information worldwide.

a. Justification

DS must ensure the Department complies with standards approved by the Overseas Security Policy Board (OSPB) and other laws and policies, as standards are a critical step in protecting personnel, property, and information domestically and abroad.

Bureau Objective 1.2: Lead in the protective operations field by collecting, publishing, and implementing continuous improvements based on lessons learned, and defining and demonstrating best practices.

a. Justification

DS must continue to be a world-class leader in protective operations by providing protection, overseas and domestically, to the Secretary of State and other U.S. government officials, foreign dignitaries, and foreign Diplomatic personnel and missions. To provide leadership and continuous process improvement, DS must be

able to collect lessons learned and best practices, apply these to training and operations, and share this information with other U.S. and foreign partners.

Bureau Objective 1.3: Leverage intelligence information and timely access to resources to operate safely and effectively, particularly in significant threat areas and critical situations.

a. Justification

DS plays a critical role in enabling the Department to conduct diplomatic engagement in dangerous and unstable locales. To succeed, DS must have access to real-time threat intelligence, quickly disseminate this information to the field, and employ the appropriate equipment and systems to mitigate security vulnerabilities.

Bureau Objective 1.4: Protect networks, IT assets, and information from cyber threats.

a. Justification

Confidentiality, integrity, and availability of the Department's information are vital to the interests of the United States and its compromise is a major security threat, which can affect the safety of personnel, facilities, and operations. Securing information technology is critical to current and future operations of the Department. DS must be able to detect, react, and respond to threats and vulnerabilities through 24/7 global network monitoring, cybersecurity assessments, cyber threat intelligence sharing, and penetration testing. DS must also establish a situational awareness baseline to annually evaluate the Department's cyber security posture. DS has a robust cyber security strategy to identify threats, protect assets, detect and respond to incidents, and develop plans for post-incident recovery.

Bureau Objective 1.5: Prevent harm from insider threats by identifying those whose actions intentionally or unintentionally pose risk to the Department and its assets.

a. Justification

Compromise of the Department's assets, networks, and information by insiders is a major vulnerability. The insiders may be malicious actors or careless employees. Counteracting insider threats allows DS to provide a more secure environment for the conduct of diplomacy.

Bureau Goal 2: Protect the homeland and the integrity of U.S. travel documents through effective and efficient investigations to prevent harm to the United States and its citizens from criminal and terrorist activity.

a. Description and Linkages

DS plays a critical role in protecting the homeland through enforcement of statutes related to U.S. travel document fraud. DS must ensure its investigative agents have the right resources and knowledge, including familiarity with emerging travel document fraud trends. In recent years, travel document fraud also has proven to be an enabling offense for transnational crime such as terrorism, narcotics smuggling, and human trafficking. This goal is in line with Goal 1, Objective 1.5 of the State/USAID JSP and the National Security Strategy.

b. Key Partners and Stakeholders

Countermeasures (DS/C), Domestic Operations (DS/DO), and Training (DS/T).

Bureau Objective 2.1: Leverage all resources and stakeholders for investigating U.S. passport and visa fraud to successfully refer cases to support Department priorities.

a. Justification

To protect the homeland and the integrity of U.S. travel documents, DS must refer cases successfully and achieve the greatest output from its agents and law enforcement partners. It must also maximize its own efficiency while leveraging other stakeholders as needed.

Bureau Objective 2.2: Conduct high-quality and efficient investigations that protect the integrity of U.S. travel documents.

a. Justification

DS must ensure agents refer high-quality cases to prosecutors. Doing so also requires making sure agents understand what types of cases will be accepted for prosecution, so they can dedicate their time and resources to have the greatest impact.

Bureau Objective 2.3: Support investigations of U.S. travel document fraud by strengthening investigative capacity.

a. Justification

Since threat actors attempt to obtain U.S. passports and visas at overseas posts with fraudulent documents from foreign governments, DS needs to counter fraud at its source outside the United States with the help of host countries.

Bureau Goal 3: Provide high-quality training to equip Department and other U.S. government personnel engaged in U.S. foreign affairs, as well as Department dependents, with the right skills to safely and successfully operate in the current threat environment.

a. Description and Linkages

DS is a leader in security training and it must ensure its workforce and related stakeholders have the skills to respond to the changing nature of the threat environment worldwide. To operate efficiently and achieve cost savings, DS will need to consolidate most of its hard-skills training into one location. The Bureau must also coordinate with all directorates to ensure courses reflect the current threat and operating environments. This goal is linked to Performance Goal 4, Objective 4.3 of the State/USAID JSP, the recommendations of the Benghazi Accountability Review Board (ARB), and the Department of State, Foreign Operations, and the Related Programs Appropriations Act 2008 (Div. J, P.L. 110-161).

b. Key Partners and Stakeholders

Countermeasures (DS/C), Cyber and Technology Security (DS/CTS), Domestic Operations (DS/DO), Executive Director (DS/EX), High Threat Programs (DS/HTP), International Programs (DS/IP), Threat Investigations & Analysis (DS/TIA), Security Infrastructure (DS/SI), and Training (DS/T).

Bureau Objective 3.1: Consolidate hard-skills training at the Foreign Affairs Security Training Center (FASTC) to improve training efficiency and achieve cost efficiencies.

a. Justification

Consolidating hard-skills training and personnel at FASTC will give DS more centralized control over its training curriculum while increasing efficiencies.

Bureau Objective 3.2: Ensure that DS and Department workforce is consistently trained and capable of meeting the challenges posed by the current threat environment.

a. Justification

DS ensures that its training is specific to the unique threat environment faced in the field by its own workforce, as well as Department and other U.S. government personnel assigned overseas.

Bureau Objective 3.3: Provide a management system for training to align resources to priorities for effective human capital planning.

a. Justification

Training is a major investment in human capital and a learning management system is needed to ensure personnel have the most up to date training and skills.

Bureau Goal 4: Invest in a skilled, dedicated, trusted, diverse, and inclusive workforce to realize the mission of DS more effectively.

a. Description and Linkages

DS is investing in a workforce, from contractors to federal employees, which can grow and adapt to the demands of an evolving threat environment, both domestically and abroad. This requires ensuring that the people who work for the Bureau are properly vetted, comprised of diverse backgrounds, experiences, and skillsets, and their viewpoints are considered in the daily workflow. DS must also work to ensure that they retain personnel. This goal is in line with Goal 4, Objective 4.3 of the State/USAID JSP.

b. Key Partners and Stakeholders

Executive (DS/EX), Security Infrastructure (DS/SI), and Training (DS/T).

Bureau Objective 4.1: Cultivate effective leaders and managers who are trained for excellence and get the best results from their staff.

a. Justification

The success of the Bureau relies on effective leaders and managers who are equipped with the necessary skills to lead staff and manage resources. As such, managers must develop through relevant, mandatory training and be open to feedback from staff. Managers also play a key role in hiring, developing, and promoting staff, and thus play a pivotal role in creating a diverse and inclusive working environment. To ensure the DS workforce reflects the United States, managers must understand how DS and their teams are doing in furthering this effort.

Bureau Objective 4.2: Work together across DS to fill positions and align staff resources to Bureau priorities.

a. Justification

Critical to the DS mission is the ability to fill vacancies and ensure that human capital is effectively aligned with Bureau priorities. DS must pursue best practices regarding hiring and staffing to ensure the Bureau is adequately and effectively staffed.

Bureau Objective 4.3: Recruit, develop, and retain a skilled and committed workforce.

a. Justification

DS must harness technology and planning to manage the assignments of its workforce, anticipate personnel needs, and hire new employees. This includes evaluating various methods and strategies for identifying and recruiting the right staff, including those utilized by other federal organizations.

Bureau Goal 5: Harness the right technologies and business processes to innovate and safely operate in a digital environment.

a. Description and Linkages

DS deploys some of the most sophisticated technical security in the world, and is often a catalyst for technology evolution in carrying out its mission to protect U.S. personnel, facilities, and information, stateside and overseas. For DS to continue to develop the capabilities to use data and technology to become a more innovative organization, it must ensure that it can quickly adapt to the new types of technological systems that emerge, including identifying the right countermeasures against threat actors - as well as quickly procuring needed assets to provide greater visibility on Bureau operations and improve resource allocation and decision-making. This goal is in line with Goal 4, Objective 4.2 of the State/USAID JSP.

b. Key Partners and Stakeholders

Countermeasures (DS/C), Cyber and Technology Security (DS/CTS) Domestic Operations, (DS/DO), Executive (DS/EX), Front Office (DS), High Threat Programs (DS/HTP), International Programs (DS/IP), Security Infrastructure (DS/SI), Threat Investigations and Analysis (DS/TIA), and Training (DS/T).

Bureau Objective 5.1: Become a digital and data-driven organization by employing the right technology, talent, and processes to operate effectively and accomplish the mission.

a. Justification

DS can become more effective at organizing its people, processes, and technologies around becoming a digital organization. The first step in this process is to identify how systems can be strengthened, what investments need to be made, and what data is available and needed to inform decision-making.

Bureau Objective 5.2: Leverage digital tools to quickly distribute safety, threat, and other information, and communicate effectively with the public.

a. Justification

DS can better distribute unclassified intelligence and threat information through digital tools to alert stakeholders across the globe to emerging threats, including U.S. organizations and travelers abroad. It can also use digital tools to more efficiently respond to Freedom of Information Act (FOIA) requests by automating its business processes. DS must also communicate effectively with the public about its efforts to protect U.S. foreign affairs activity.

Objective 5.3: Standardize common platforms and architectures within DS to avoid duplicative IT investments and to allow for an effective IT portfolio management system.

a. Justification

Non-uniform technology platforms lead to increased operations and maintenance costs, create potential vulnerabilities, and may also prevent economies of scale in procurement. DS must understand what systems and applications are currently deployed across the Bureau and identify opportunities to deploy common platforms. DS/EX/CTO can work closely with IRM to ensure that standard platforms and processes are being used for technology investments and that DS avoids duplication.

Bureau Objective 5.4: Expand classified systems to protect sensitive, classified, and intelligence information.

a. Justification

To better realize its mission to protect sensitive information and to safeguard U.S. government personnel from threats, DS must work with the Department to build out its technical capacity to handle classified information.

4. Cross-cutting Management Goal

Cross-cutting Management Goal 6: Demonstrate strong and effective leadership and management of the Bureau to provide the foundation for an agile, proactive, and flexible security organization.

a. Description and Linkages:

Per FBS guidance, the cross-cutting management goal refers to internal Bureau functions whose efforts cut across the organization and reflect priorities of leadership. This goal and supporting objectives identify key priorities that aim to significantly improve efficiency, effectiveness, employee, and customer satisfaction, and support the achievement of broader FBS. As part of its cross-cutting management goal, DS identified that it must adopt an operating model that will enable it to adapt to a changing threat environment. This includes being able to allocate and manage resources more responsively and to simplify key business processes. The Bureau must also become more adept at framing problems and solving them creatively. This goal directly supports Goal 4, Objective 4.3 of the JSP.

b. Key Partners and Stakeholders

Countermeasures (DS/C), Cyber and Technology Security (DS/CTS), Domestic Operations (DS/DO), Executive (DS/EX), Front Office (DS), High Threat Programs (DS/HTP), International Programs (DS/IP), Security Infrastructure (DS/SI), Training (DS/T), and Threat Investigation and Analysis (DS/TIA).

Cross-cutting Management Objective 6.1: Manage Bureau finances through effective budgeting and resource allocation.

a. Justification

Effective budgeting requires the Bureau implement a robust budgeting system and ensure managers employ best practices for budgeting and cost tracking.

Cross-cutting Management Objective 6.2: Strategically enhance intra-agency relationships to enable DS to quickly leverage the authorities and capabilities of partner agencies in executing its mission.

a. Justification

As an important part of the U.S. government's global security capability, DS needs to participate in joint decision-making bodies whose policies affect the Bureau.

Cross-cutting Management Objective 6.3: Streamline the procurement process to ensure purchasing requests are met in a timely manner, especially for mission critical needs.

a. Justification

The Bureau believes the acquisitions process can be improved and DS should work with stakeholders to establish reasonable standards for procuring goods and services to fulfill its mission.

Cross-cutting Management Objective 6.4: Promote critical thinking and problem-solving skills to become a more solutions-driven organization.

a. Justification

Improved delivery by the Bureau is dependent on its employees being empowered to apply critical thinking and problem-solving skills to challenges posed by the operating environment. DS leadership, managers, and supervisors must always be supporting the workforce and their teams by discussing common ways to solve problems and sharing best practices. This will allow for innovation and excellence in providing physical security, executive protection, and information security - including in high threat areas and situations. DS employees must strive to be innovative with the resources they have before requesting more funding and personnel.

Cross-cutting Management Objective 6.5: Pursue organizational excellence through effective program performance management and leadership.

a. Justification

DS is committed to continuous improvement in strategic planning and performance management. It aims to create a data-informed approach aligning priorities to the budget processes and capturing lessons learned to improve planning. DS continues to make progress in sequencing policies and strategic plans, enabling those plans to drive the formulation of budgets and assessing performance against objectives.

Cross-cutting Management Objective 6.6: Educate and inform DS program stakeholders through effective internal and external communications.

a. Justification

Providing DS stakeholders - the general public, Department and Bureau personnel, and constituent audiences - with accurate and timely information regarding DS programs is critical to the Bureau's continued programmatic effectiveness and success.