Office of Inspector General
United States Department of State

ISP-I-22-13 | Office of Inspections | May 2022

Inspection of the Bureau of Diplomatic Security's Diplomatic Courier Service

DOMESTIC OPERATIONS

HIGHLIGHTS
Office of Inspector General
United States Department of State

ISP-I-22-13

What OIG Inspected
OIG inspected the operations of the Diplomatic Courier Service in the Bureau of Diplomatic Security.

What OIG Recommends
OIG made 4 recommendations: 3 to the Bureau of Diplomatic Security and 1 to the Bureau of Administration.

In its comments on the draft report, the Department concurred with 3 recommendations and neither agreed nor disagreed with 1 recommendation. OIG considers all 4 recommendations resolved. The Department's response to each recommendation, and OIG's reply, can be found in the Recommendations section of this report. The Department's formal response is reprinted in its entirety in Appendix B.

May 2022
OFFICE OF INSPECTIONS
DOMESTIC OPERATIONS

Inspection of the Bureau of Diplomatic Security's Diplomatic Courier Service

What OIG Found

- The Diplomatic Courier Service's Director and Deputy Director generally communicated well with staff and modeled Department of State leadership principles.
- There was a perception among some Diplomatic Courier Service staff, which had not been addressed, that favoritism was a factor in determining assignments.
- Department guidance on reporting security incidents involving classified pouches was unclear and sometimes contradictory, resulting in inconsistent reporting.
- Information systems security was not fully integrated into the Classified Pouch Modernization Effort, and the Diplomatic Courier Service did not maintain modernization project documentation in a Department-owned location.
- Spotlight on Success: The Bangkok Regional Diplomatic Courier Division created a COVID-19 Status Guide that increased efficiency in planning diplomatic courier missions by consolidating needed information on travel requirements.

CONTENTS

CONTEXT

The Bureau of Diplomatic Security, Countermeasures Directorate's Diplomatic Courier Service (DS/C/DC) ensures secure delivery of classified and sensitive material between the Department of State (Department) and U.S. diplomatic missions worldwide. A diplomatic courier's primary duty is to ensure the inviolability of classified pouches and their unbroken chain of custody while crossing international borders or at any time the courier is in control of diplomatic material. DS/C/DC supports more than 30 Department entities and other Federal agencies around the world and the Secretary of State's global travel. Established in 1918 to improve mail and message delivery during World War I, DS/C/DC uses various methods of conveyance, including by road, sea, and air. Annually, it is responsible for delivering more than 5 million pounds of classified and sensitive material across international borders in accordance with Article 27 of the Vienna Conventions on Diplomatic and Consular Relations.

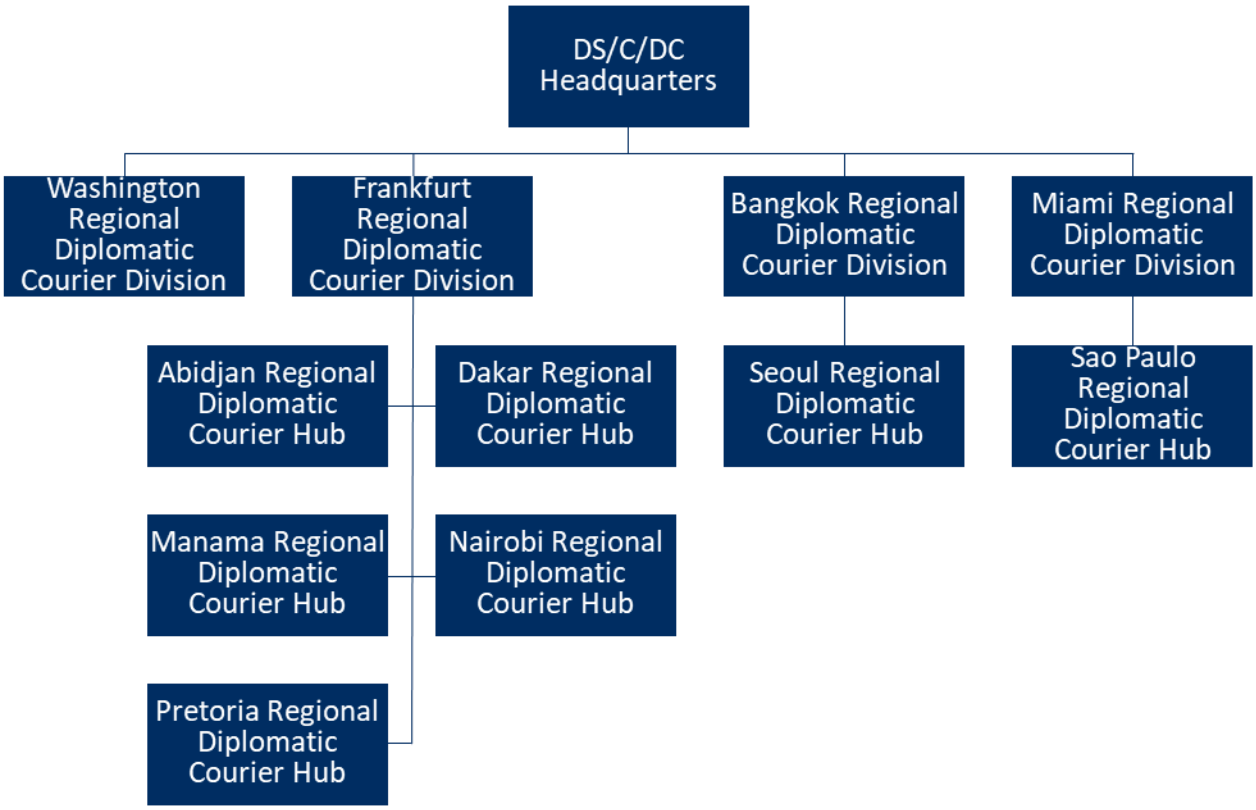
The DS/C/DC organization, as shown in Figure 1, consists of a Headquarters office and the Washington Regional Diplomatic Courier Division, both located in the Washington, D.C. area; Regional Courier Divisions in Frankfurt, Germany; Miami, Florida; and Bangkok, Thailand; and Courier Hub Offices sited in Abidjan, Côte d'Ivoire; Dakar, Senegal; Manama, Bahrain; Nairobi, Kenya; Pretoria, South Africa; Seoul, South Korea; and Sao Paulo, Brazil.

At the time of the inspection, DS/C/DC had 104 authorized U.S. direct-hire positions, 22 eligible family members, and 33 locally employed staff. The diplomatic courier profession is a specialist career track in the Foreign Service. Of the 104 U.S. direct-hire positions, 2 were Senior Foreign Service, 5 were FS-01, and 9 were FS-02.[1] DS/C/DC also coordinates the work of non-professional couriers.[2]

[1] The Foreign Service pay scale for non-Senior Foreign Service employees comprises nine pay grades, with FS-01 being the highest.

[2] Non-professional couriers are U.S. Government employees who possess a Top Secret clearance and are provided with official documentation to transport diplomatic pouches in emergencies or when a diplomatic courier cannot provide the required service.

Figure 1: DS/C/DC Organizational Chart



Source: OIG generated from information obtained from DS/C/DC.

OIG evaluated the office's executive direction, impact of the COVID-19 pandemic on operations, security operations, resource management, and information management operations consistent with Section 209 of the Foreign Service Act of 1980.[3]

EXECUTIVE DIRECTION

OIG assessed DS/C/DC's leadership based on interviews that included comments on its leadership team, a review of OIG questionnaires completed by DS/C/DC staff and other documents, and observation of activities during on-site inspection work.

DS/C/DC's leadership consisted of a Director and Deputy Director. The Director who led DS/C/DC at the beginning of the inspection retired from the Department in October 2021,

[3] See Appendix A.

before the inspection's conclusion. In November 2021, a new Director assumed DS/C/DC leadership. The new Director, a 22-year veteran of DS/C/DC, had most recently served as the head of DS/C/DC's Frankfurt Regional Diplomatic Courier Division. During his career, the new Director had also previously served as the DS/C/DC Director from 2016 to 2019, as well as in other DS/C/DC positions both in Washington and overseas. The Deputy Director joined the Front Office in August 2019, and his previous DS/C/DC assignments included Manama, Bahrain; Washington, D.C.; Sao Paulo, Brazil; Frankfurt, Germany; and Bangkok, Thailand.

OIG found that the recently retired DS/C/DC Director and the Deputy Director generally modeled the Department's leadership and management principles set forth in 3 Foreign Affairs Manual (FAM) 1214. The Director and the Deputy Director complemented each other, with the Director focusing on strategic priorities and the Deputy Director managing daily operational requirements of DS/C/DC. The new Director said he expects this division of labor with the Deputy Director to continue.

Leadership Communicated Effectively With Employees

The Director and Deputy Director effectively communicated with the DS/C/DC staff in accordance with 3 FAM 1214 b(4). They established several methods of communications with the four regional divisions and seven hub offices. For example, the Director established monthly leadership calls to the regional directors and the deputy regional directors to share relevant information. The Director supplemented this dialogue with weekly telephone calls to each regional director to discuss important topics.

The DS/C/DC Front Office also shared information with DS/C/DC staff through the distribution of Weekly Activity Reports posted on its intranet site, the distribution of Quarterly Performance Reports, daily situation reports submitted by each Regional Division, and mass emails to communicate with all DS/C/DC staff, including discussions of leadership tenets. To obtain feedback on DS/C/DC operations, the Director and Deputy Director encouraged diplomatic couriers to visit them in their offices and to email them directly. The Director and Deputy Director also obtained feedback by asking their customers for their perspectives on DS/C/DC operations.

Office Needed to Address Perceptions of Favoritism in Assignments Process

Senior leaders raised with OIG concerns that there was a perception of favoritism in DS/C/DC with respect to the assignments process. To determine assignments, diplomatic couriers bid on and expressed interest in open positions. DS/C/DC senior leaders then discussed who should be assigned to what position and made recommendations to a DS panel. That panel submitted final recommendations to the Bureau of Global Talent Management, which made final assignments. However, while DS/C/DC senior leaders stated their recommendations were based on diplomatic courier preferences along with mission needs, the factors for consideration were not written and were not well-known to staff.

Through interviews with DS/C/DC staff, OIG confirmed that there was a perception among some, but not all, diplomatic couriers that favoritism was a factor when DS/C/DC senior staff prepared post assignments of diplomatic couriers. Related to this perception was that favorable assignments could contribute to some couriers being able to better demonstrate their competency for promotion. Some staff noted rumors of favoritism while others said they had been warned about favoritism, perpetuating the perception in the organization. OIG noted that the problem was exacerbated by the fact that DS/C/DC leadership had not addressed the issue directly with employees by transparently sharing the process for making assignments or by stating its commitment to making decisions on courier assignments free of favoritism.

According to 3 FAM 1214b(1), (4), and (9), Department employees should model integrity, be cognizant of the morale and attitude of employees, and encourage an atmosphere of open dialogue and trust. Senior leaders, including the Director and the Deputy Assistant Secretary above him, acknowledged that the perception of favoritism was a serious issue and one that they wanted to remediate even though they had not previously addressed it directly. Failing to address perceptions of favoritism can undermine employee confidence, morale, and trust in the organization.

> **Recommendation 1:** The Bureau of Diplomatic Security should require Diplomatic Courier Service leadership to develop and share its process for courier assignments with all employees including the commitment that decisions will be made free of favoritism. (Action: DS)

Mentoring First- and Second-Tour Diplomatic Couriers

DS/C/DC does not have a formal mentoring program for its first- and second-tour diplomatic couriers. DS/C/DC relied on informal mentoring programs at regional divisions and hubs in which experienced diplomatic couriers volunteered to guide and assist first- and second-tour diplomatic couriers. In addition to one-on-one advice from an experienced diplomatic courier, the informal mentoring programs included being paired with an experienced diplomatic courier for one or more trips to gain practical experience. Some diplomatic couriers told OIG that they believed the informal mentoring programs worked well, but others expressed a desire for a more formal mentoring program. Department guidance in 3 FAM 1214b(8) makes embracing mentoring and other means to develop talent a core precept of the Department's leadership and management principles.

Given the wide range of views among the diplomatic couriers on informal mentoring, OIG brought these issues to the new Director's attention. In response, the Director stated he intended to quickly establish a service-wide mentor policy that detailed how every diplomatic courier could be mentored in a consistent fashion during their first two tours. In addition to being paired with experienced diplomatic couriers on their first few trips, the Director said that first- and second-tour diplomatic couriers would be assigned a mentor at their posts and have regular meetings with supervisors to discuss issues of importance and promote learning.

IMPACT OF COVID-19 PANDEMIC ON OPERATIONS

With the onset of the COVID-19 pandemic, the Department significantly limited DS/C/DC's missions to those that were critical to life safety or to U.S. national security. Many countries implemented quarantine requirements, airlines decreased the number of commercial aircraft available to carry cargo, and airlines started using aircraft with smaller cargo capacity, creating major challenges to DS/C/DC's normal delivery operations. In mid-March 2020, DS/C/DC stopped operating its normal missions, and any proposed diplomatic courier deliveries had to be approved by the Deputy Assistant Secretary for Countermeasures and the Executive Director in Diplomatic Security. Each shipment required a special justification and a general description of what the pouches contained.

Quarantine requirements made it very difficult for diplomatic couriers to execute deliveries, especially in Asia, where countries had strict quarantine policies. For example, Thailand required a 2-week hotel quarantine after entry into the country. Additionally, due to entry restrictions, diplomatic couriers took the next return flight after a delivery on trips that would typically include an overnight stay. In OIG interviews, diplomatic couriers described how the need for frequent COVID testing and corresponding paperwork requirements, along with frequently changing and short-notice trips, created challenging situations that were difficult to navigate. At times, these challenges negatively affected morale.

Despite the limitations and hardships attributable to the pandemic, DS/C/DC achieved some important successes. Working closely with the Bureau of Medical Services, starting in December 2020, DS/C/DC delivered COVID vaccines and associated medical equipment throughout the world. DS/C/DC also supported Embassy Moscow after the closure of two U.S. consulates in Russia, delivered a modular building by ship to Jerusalem for the embassy's new office building, and supported the drawdown and evacuation of material from Embassy Kabul.

Spotlight on Success: COVID-19 Status Guide Increased Efficiency in Planning Diplomatic Courier Missions During Pandemic

The Diplomatic Courier Service's Bangkok Regional Diplomatic Courier Division created a weekly COVID-19 status reference guide to provide diplomatic couriers with updated country-specific COVID-19 requirements for 32 countries throughout Asia and the Pacific. The guide provided information such as testing timelines and types of tests accepted, required documents, and quarantine guidelines. The guide consolidated data from multiple government agencies and data sources that diplomatic couriers would otherwise have had to research independently. Diplomatic courier staff throughout the region were able to use this guide to better prepare for mission critical diplomatic pouch trips, thereby minimizing unexpected travel disruptions.

SECURITY OPERATIONS

OIG reviewed DS/C/DC's security operations, including the couriers' adherence to policies and processes for maintaining control of classified diplomatic pouches and for reporting security incidents involving classified pouches. OIG found that DS/C/DC generally met 12 FAM 120 and 130 requirements for maintaining control and ensuring the inviolability of classified diplomatic pouches. However, with respect to reporting security incidents involving classified pouches, OIG found that the Department's guidance on reporting such incidents was unclear and sometimes contradictory, resulting in nonstandard compliance, as discussed below.

Guidance on Reporting Security Incidents Involving Classified Pouches Was Unclear

OIG determined that Department guidance on reporting security incidents involving classified pouches was unclear and sometimes contradictory in two areas: which classified pouch security incidents should be reported and what mechanisms should be used to do the reporting. Department guidance identifies three specific types of security incidents involving classified pouches: classified pouch breaches, classified pouch security incidents,[4] and pouch out-of-control incidents.[5]

However, these three types of similar-sounding security incidents are not clearly described in one location in Department guidance. In addition, across different sets of guidance, the terms appear to be used interchangeably, making it unclear what the reporting requirements are for a particular type of incident. For example, 12 FAM 130 identifies the scope of its application to classified pouch breaches and classified pouch security incidents but only describes potential situations and reporting responsibilities for classified pouch breaches.[6] It is silent on reporting responsibilities, if any, for classified pouch security incidents. Furthermore, 12 FAM 130 does not specifically define pouch out-of-control incidents, although the term pouch out-of-control incident is defined in 12 FAM 013, which is a list of "Definitions of Diplomatic Security Terms." But neither classified pouch breaches nor classified pouch security incidents appear on that list of terms. In addition, OIG was unable to identify any reporting responsibilities in either FAM or Foreign Affairs Handbook (FAH) guidance for pouch out-of-control incidents.

[4] According to 12 FAM 131, a "classified pouch breach" and a "classified pouch security incident" situation include an interruption of cleared U.S.-citizen custody that may result in unauthorized individuals gaining access to a classified diplomatic pouch. Examples of "classified pouch breaches" include, but are not limited to, missing classified diplomatic pouches, lost classified pouches, and/or unauthorized opening of classified diplomatic pouches. Examples of a "classified pouch security incident" include the use of X-ray, canine scent detection, metal detectors, contact explosive detection, or any other circumstance that may risk the inviolability of the classified diplomatic pouch.

[5] According to 12 FAM 013, a "pouch out-of-control" incident is any situation where cleared U.S. citizen control over a classified pouch is interrupted for any period of time making outside intervention and compromise of its contents a possibility.

[6] 12 FAM 130, "Classified Pouch Breaches" is comprised of four sections – 12 FAM 131, "Applicability," 12 FAM 132, "Responsibilities," 12 FAM 133 "Investigations," and 12 FAM 134 "Disciplinary Action."

In addition to FAM and FAH guidance, in 2019, DS/C/DC issued Policy Memorandum 19-03 to provide guidance to couriers in the event of a classified pouch breach.[7] That memorandum also defines "classified diplomatic pouch security incidents" and "classified diplomatic pouch out-of-control incidents," but only the definition of the first term aligns with the definition of the same term in the FAM. For pouch out-of-control, the policy memorandum states it "includes, but is not limited to, missing classified diplomatic pouches, lost classified diplomatic pouches, unauthorized opening of classified diplomatic pouches." However, this definition is what the FAM identifies as a classified pouch breach. In terms of incident reporting, the policy memorandum incorrectly lists responsibilities of personnel involved in pouch out-of-control incidents as the same responsibilities listed in 12 FAM 130 for classified pouch breaches. As noted in the above paragraph, 12 FAM 130 does not address pouch out-of-control incidents. The inconsistent terminology in Department guidance makes it difficult to determine which security incidents are required to be reported.

The mechanics of how to report a security incident are also not clear in Department guidance. Guidance in 12 FAM 130 and in Policy Memorandum 19-03 generally describes two different types of reporting mechanisms for diplomatic couriers. The first mechanism involves contacting certain individuals and organizations in the event of a security incident. Both sets of guidance are clear that diplomatic couriers must contact the Regional Security Officer (RSO) where the incident occurred. However, the two sets of guidance do not fully align on who else the diplomatic courier must contact.[8] Additionally, both sets of guidance are silent on how contact should be made, leaving it to the courier's discretion. The second reporting mechanism discussed in Department guidance is preparing spot reports.[9] Because there is no common format for spot reports, Policy Memorandum 19-03 includes a spot report template to use when reporting a classified pouch security incident to the RSO where the incident occurred, which is in addition to the requirement to contact the RSO noted earlier. Both sets of guidance state that the RSO is then responsible for investigating the incident and submitting the spot report to the Bureau of Diplomatic Security (DS) Command Center.

In interviews with OIG, diplomatic couriers gave differing descriptions of their understanding of the mechanism to report a classified pouch security incident. For example, some diplomatic couriers reported incidents to their supervisors via phone or email. Some diplomatic couriers used the Courier Travel System[10] to capture incidents, such as a temporary loss of visual control, that either the diplomatic courier or their supervisor determined did not require a spot report. In such instances, couriers and supervisors relied on their judgment because

[7] Bureau of Diplomatic Security, Diplomatic Courier Service Policy Memorandum 19-03, "Guidance for Classified Pouch Breaches," December 18, 2019.

[8] Between the guidance in 12 FAM 130 and DS/C/DC Policy Memorandum 19-03, the diplomatic courier must also contact the information programs officer at the post where the incident occurred, the operations officer responsible for the trip, the nearest regional diplomatic courier officer, and/or DS/C/DC.

[9] Spot reports are used throughout DS as a tool to communicate the basic facts of a security incident to management, security officials, and program officers.

[10] The Courier Travel System is used by DS/C/DC to schedule, process, and report on all trips electronically.

Department guidance was unclear on what the threshold was for an incident to be reported via a spot report.

The lack of clarity about which pouch security incidents needed to be reported, combined with the lack of standardized mechanisms for reporting those incidents, meant that DS/C/DC leadership, which had ultimate responsibility for managing the courier program, did not consistently receive reports of pouch security incidents. OIG determined, for example, that DS/C/DC leadership did not have in their records any of the five spot reports submitted to the DS Command Center from FY 2019 through FY 2021. To compound reporting problems, RSOs entered spot reports into a system maintained by the DS Command Center. However, no DS/C/DC staff, including leadership, had access to that information because data in the DS Command Center-maintained system was considered law enforcement sensitive and was not widely available outside the Command Center itself. Because it did not consistently receive reporting on classified pouch security incidents, DS/C/DC leadership was not able to identify trends or vulnerabilities and put measures in place to prevent future classified pouch security incidents.

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, should require the Diplomatic Courier Service to revise and disseminate Foreign Affairs Manual and internal Diplomatic Courier Service guidance to clarify (1) what types of classified pouch security incidents must be reported and (2) the mechanisms diplomatic couriers must use to report the incidents. (Action: DS, in coordination with A)

INFORMATION MANAGEMENT

OIG reviewed DS/C/DC's information management operations, which predominantly centered on the Classified Pouch Modernization Effort (CPME), a multi-year, multi-million-dollar project to modernize DS/C/DC's business processes with new technology to increase efficiency and accountability. The CPME initiative, which began in 2014, involves personnel from the Bureau of Administration, DS/C/DC, and a contractor undertaking development work using systems owned by the Bureau of Administration. At the time of the inspection, diplomatic couriers were using several CPME components to perform their work, as follows:

- Courier Mobile Application – The application was deployed to all classified mail hubs in 2016 and was designed to be used with Department-approved mobile phones. The application helps diplomatic couriers manage their trips and enhance pouch accountability while they are on the go by leveraging the existing Diplomatic Pouch and Mail module and the Courier Travel System module in the Bureau of Administration's Integrated Logistics Management System (ILMS).[11]

[11] The Diplomatic Pouch and Mail module facilitates shipment, tracking, and receiving of diplomatic pouches between posts or between domestic locations and posts. The Integrated Logistics Management System provides end-to-end logistics and supply chain services for the Department.

- Centralized Schedule Board – Deployed in 2018 and built within the Bureau of Administration's myServices[12] platform, the Centralized Schedule Board is used by diplomatic couriers to centralize route information and mission scheduling across 12 regional offices. It also stores diplomatic couriers' passport and visa information.
- Handheld scanners – The scanners are an integral part of CPME, as the diplomatic couriers use them to scan pouches.

During the inspection, OIG found two areas of the CPME initiative that required management attention, as described below.

Information Systems Security Was Not Fully Integrated into the Classified Pouch Modernization Effort

Information systems security was not fully integrated into the CPME initiative. Guidance in 5 FAM 824(3) and (4) requires information systems security officers (ISSOs) to work closely with system administrators to ensure all security related functions and activities are performed and to play a leading role in identifying, evaluating, and minimizing risk to all IT systems. However, OIG found that an ISSO from the Bureau of Administration[13] did not attend CPME system development meetings, nor did they review changes and updates to CPME applications on a regular basis. Furthermore, Bureau of Administration information security personnel told OIG that the Courier Mobile Application was within the ILMS system security authorization boundary,[14] but OIG reviews of the ILMS system security plan found no mention of the Courier Mobile Application.

OIG determined that information systems security was not fully integrated into the CPME initiative because the Bureau of Administration and DS did not agree on which bureau should be responsible for information systems security of CPME applications. According to 12 FAM 613.4, the designated application ISSO team is responsible for implementing 12 FAM 600 information security technology policies and procedures on designated information systems. This would place responsibility on the Bureau of Administration, which is the designated application ISSO team for CPME applications. However, information security personnel in the Bureau of Administration told OIG that security oversight should be DS's responsibility because CPME applications support diplomatic courier business processes. Furthermore, DS's information security personnel told OIG that security oversight was not their responsibility because DS was not the system owner for CPME applications. The lack of ISSO involvement and integration in the CPME initiative increases the risk of the Department's information being compromised or operations disrupted due to inadequate security controls.

[12] myServices is a modernized, web-based enterprise service management solution that uses industry-leading, commercial off-the-shelf enterprise service management software.

[13] According to iMatrix, the system owner for the Courier Mobile Application and the Centralized Schedule Board is the Bureau of Administration.

[14] A security authorization boundary is all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Recommendation 3: The Bureau of Administration, in coordination with the Bureau of Diplomatic Security, should establish a process for an information systems security officer team to review and approve development work and changes to Classified Pouch Modernization Effort applications for security compliance. (Action: A, in coordination with DS)

Lack of a Central Location in the Department for Classified Pouch Modernization Effort Project Documentation

DS/C/DC did not maintain CPME project documentation in a central Department location. Staff in DS/C/DC and in the Bureau of Administration told OIG that personnel working on CPME depended on the contractor for copies of project documentation for review and approval since there was no central Department repository. In accordance with 5 FAH-4 H-211a, the Department must create and preserve records containing adequate and proper documentation of the organization, policies, decisions, and essential operations of the Department. To ensure the appropriate preservation of records, each bureau and office must also organize and maintain documentary materials that it produces or receives.

DS/C/SC staff performed CPME responsibilities as collateral duties along with other office responsibilities, with the CPME lead role rotating among staff who were assigned to the Headquarters office. Due to CPME responsibilities being collateral duties, staff were not familiar with the risks associated with the lack of a central repository. DS/C/DC's lack of ownership and retention of project documentation risks the loss of institutional knowledge for the Department on the CPME initiative, especially with the constant rotation of staff managing and leading the effort.

Recommendation 4: The Bureau of Diplomatic Security should require the Diplomatic Courier Service to maintain Classified Pouch Modernization Effort project documentation in a central location on the Department network. (Action: DS)

RESOURCE MANAGEMENT

OIG evaluated DS/C/DC administrative processes for resource management by reviewing records related to property management and inventory, vehicle fleet management—including vehicle inventory, driver safety and medical certifications, and DriveCam compliance—premium class travel authorizations, contracts, and unliquidated obligations. OIG found that DS/C/DC generally implemented required processes and procedures in accordance with applicable laws and Department guidance.

RECOMMENDATIONS

OIG provided a draft of this report to Department stakeholders for their review and comment on the findings and recommendations. OIG issued the following recommendations to the Bureau of Diplomatic Security and the Bureau of Administration. The Department's complete response can be found in Appendix B.[1, 2]

Recommendation 1: The Bureau of Diplomatic Security should require Diplomatic Courier Service leadership to develop and share its process for courier assignments with all employees including the commitment that decisions will be made free of favoritism. (Action: DS)

Management Response: In its April 19, 2022, response, the Bureau of Diplomatic Security neither agreed nor disagreed with this recommendation. The bureau acknowledged the perception of favoritism in the courier assignment process and that it remained committed to Department policy on the assignment process. The bureau noted it has agreed to partner with the Bureau of Global Talent Management to use the iMatch software in the assignments process for certain skill codes, including the Diplomatic Courier Service.

OIG Reply: OIG considers the recommendation resolved. OIG acknowledges the Bureau of Diplomatic Security's plans to partner with the Bureau of Global Talent Management to improve the courier assignment process. Additionally, as noted in the report, OIG found that the perception of favoritism in the courier assignment process was exacerbated by the fact that Diplomatic Courier Service leadership had not addressed the issue directly with employees by sharing the process for making assignments or by stating its commitment to making decisions on courier assignments free of favoritism. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Diplomatic Security required Diplomatic Courier Service leadership to develop and share its process for courier assignments with all employees including the commitment that decisions will be made free of favoritism.

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, should require the Diplomatic Courier Service to revise and disseminate Foreign Affairs Manual and internal Diplomatic Courier Service guidance to clarify (1) what types of classified pouch security incidents must be reported and (2) the mechanisms diplomatic couriers must use to report the incidents. (Action: DS, in coordination with A)

Management Response: In its April 19, 2022, response, the Bureau of Diplomatic Security concurred with this recommendation.

[1] OIG faced delays in completing this work because of the COVID-19 pandemic and resulting operational challenges. These challenges included the inability to conduct most in-person meetings, limitations on our presence at the workplace, difficulty accessing certain information, prohibitions on travel, and related difficulties within the agencies we oversee, which also affected their ability to respond to our requests.
[2] The Bureau of Diplomatic Security and the Bureau of Administration submitted a combined response to the draft report.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Diplomatic Security required the Diplomatic Courier Service to revise and disseminate Foreign Affairs Manual and internal Diplomatic Courier Service guidance to clarify (1) what types of classified pouch security incidents must be reported and (2) the mechanisms diplomatic couriers must use to report the incidents.

Recommendation 3: The Bureau of Administration, in coordination with the Bureau of Diplomatic Security, should establish a process for an information systems security officer team to review and approve development work and changes to Classified Pouch Modernization Effort applications for security compliance. (Action: A, in coordination with DS)

Management Response: In its April 19, 2022, response, the Bureau of Administration concurred with this recommendation.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Administration established a process for an information systems security officer team to review and approve development work and changes to Classified Pouch Modernization Effort applications for security compliance.

Recommendation 4: The Bureau of Diplomatic Security should require the Diplomatic Courier Service to maintain Classified Pouch Modernization Effort project documentation in a central location on the Department network. (Action: DS)

Management Response: In its April 19, 2022, response, the Bureau of Diplomatic Security concurred with this recommendation. The bureau noted an expected completion date of June 2022.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Diplomatic Security required the Diplomatic Courier Service to maintain Classified Pouch Modernization Effort project documentation in a central location on the Department network.

PRINCIPAL OFFICIALS

Title	Name	Arrival Date
Director	Todd Ziccarelli[a]	8/2019
Director	Jose “Eddie” Salazar	11/2021
Deputy Director	John Wright	8/2019

[a] Todd Ziccarelli retired during the inspection and was succeeded by Jose “Eddie” Salazar.

Source: Generated by OIG from data provided by DS/C/DC.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This inspection was conducted from August 30 to December 29, 2021, in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2020 by the Council of the Inspectors General on Integrity and Efficiency, and the Inspections Handbook, as issued by the Office of Inspector General (OIG) for the Department and the U.S. Agency for Global Media (USAGM).

Objectives and Scope

The Office of Inspections provides the Secretary of State, the Chief Executive Officer of USAGM, and Congress with systematic and independent evaluations of the operations of the Department and USAGM. OIG's specific objectives for this inspection of the Bureau of Diplomatic Security's Diplomatic Courier Service (DS/C/DC) were to determine whether:

- COVID-19 affected DS/C/DC's operations and internal controls.
- COVID-19 related telework affected mission accomplishment, customer service to the public, and employee performance.
- DS/C/DC leadership led by example and cultivated the Department leadership and management principles, particularly with respect to communication among leadership and staff, as well as mentoring and staff development.
- DS/C/DC adhered to pouch security processes including maintaining control of diplomatic pouches and reporting on any breaches.
- DS/C/DC complied with records management lifecycle policies for file creation, maintenance and use, and disposition.
- The information technology systems that DS/C/DC developed as part of the Classified Pouch Modernization Effort complied with system development life cycle and information security risk assessment requirements.
- DS/C/DC adhered to the requirements for processing and approving travel authorizations that include premium class air travel.

Methodology

OIG used a risk-based approach to prepare for this inspection. Due to the COVID-19 pandemic and taking into consideration relevant guidance, OIG conducted some of the inspection remotely and in some cases, relied on audio- and video-conferencing tools in lieu of in-person interviews with Department and other personnel. OIG performed some of the inspection on site in Frankfurt, Germany; Miami, Florida; and the Washington, D.C. area. OIG also reviewed pertinent records; circulated surveys and compiled the results; and reviewed the substance of this report and its findings and recommendations with offices, individuals, and organizations affected by the review. OIG used professional judgment and analyzed physical, documentary, and testimonial evidence, to develop its findings, conclusions, and actionable recommendations.

APPENDIX B: MANAGEMENT RESPONSE

United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

April 19, 2022

TO: OIG – Sandra Lewis, Assistant Inspector General for Inspections

FROM: DS – Gentry O. Smith
A – Alaina Teplitz

SUBJECT: Response to Draft OIG Report – Inspection of the Bureau of Diplomatic Security's Diplomatic Courier Service, ISP-I-22-13

The Bureau of Diplomatic Security and the Bureau of Administration have reviewed the draft OIG inspection report. We provide the following comments in response to the recommendations provided by OIG:

OIG Recommendation 1: The Bureau of Diplomatic Security should require Diplomatic Courier Service leadership to develop and share its process for courier assignments with all employees including the commitment that decisions will be made free of favoritism. (Action: DS)

DS Response (4/19/2022): The Bureau of Diplomatic Security (DS) acknowledges the perception of favoritism in the courier assignment process within the cohort of diplomatic couriers. DS remains committed to Department policy on the assignment process. DS has agreed to partner with the Bureau of Global Talent Management (GTM) in utilizing the iMatch software in the assignments process of certain skill codes, including the Diplomatic Courier Service. The expected completion is Summer 2022 for bids on the Summer 2023 cycle.

OIG Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, should require the Diplomatic Courier Service to revise and disseminate Foreign Affairs Manual and internal Diplomatic Courier Service guidance to clarify (1) what types of classified pouch security incidents must be reported and (2) the mechanisms diplomatic couriers must use to report the incidents. (Action: DS, in coordination with A)

DS Response (4/19/2022): DS concurs with the recommendation. DS, in coordination with the Bureau of Administration (A), will require the Diplomatic Courier Service to revise and disseminate Foreign Affairs Manual (FAM) and internal Diplomatic Courier Service guidance to clarify (1) what types of classified pouch security incidents must be reported and (2) the mechanisms diplomatic couriers must use to report the incidents. As part of its plan in implementing this recommendation, the Diplomatic Courier Service has posted guidance on reporting security incidents to its SharePoint site, including citations to 12 FAM 130 and who must be notified and involved in the investigation process. A policy memorandum on security incidents is being updated to reflect consistencies in terminology. The Diplomatic Courier Service will review and update the language of relevant sections of the FAM and put forth its recommendations through the formal clearance process. The Diplomatic Courier Service expects a draft FAM update to be completed in coordination with A and ready for Countermeasures Directorate clearance by July 2022.

UNCLASSIFIED

OIG Recommendation 3: The Bureau of Administration, in coordination with the Bureau of Diplomatic Security, should establish a process for an information systems security officer team to review and approve development work and changes to Classified Pouch Modernization Effort applications for security compliance. (Action: A, in coordination with DS)

A Response (4/5/2022): The Bureau of Administration concurs with the recommendation. The A Bureau ISSO security team will include Classified Pouch Modernization Effort (CPME) system changes as part of the ILMS system security plan and reviews for security compliance.

OIG Recommendation 4: The Bureau of Diplomatic Security should require the Diplomatic Courier Service to maintain Classified Pouch Modernization Effort project documentation in a central location on the Department network. (Action: DS)

DS Response (4/19/2022): DS concurs with the recommendation. DS will require the Diplomatic Courier Service to maintain Classified Pouch Modernization Effort project documentation in a central location on the Department network. The expected completion date is June 2022.

ABBREVIATIONS

CPME	Classified Pouch Modernization Effort
DS	Bureau of Diplomatic Security
DS/C/DC	Bureau of Diplomatic Security, Countermeasures Directorate's Diplomatic Courier Service
FAH	Foreign Affairs Handbook
FAM	Foreign Affairs Manual
ILMS	Integrated Logistics Management System
ISSOs	Information Systems Security Officers
RSO	Regional Security Officer

OIG INSPECTION TEAM MEMBERS

Ken Gross, Team Leader
Thea Calder, Team Manager
Matthew Conger
Brett Fegley
Leo Hession
Jessica McTigue
Vandana Patel
Gerald Perez
Brian Roundy
Joseph Talsma

Other Contributors
Dolores Adams
Leslie Gerson
Kathryn McMahon

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926
www.stateoig.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Coordinator to learn more about your rights.
WPEAOmbuds@stateoig.gov