Office of Inspector General
United States Department of State

ISP-I-24-19 | Office of Inspections | June 2024

Review of the Bureau of Diplomatic Security's Physical Security Waivers and Exceptions Processes

TARGETED REVIEW

Summary of Review

Department of State (Department) physical security requirements—as set forth in the Secure Embassy Construction and Counterterrorism Act of 1999 (SECCA) and the Overseas Security Policy Board (OSPB) security standards—are in place to reduce risk and vulnerabilities to facilities under chief of mission (COM) authority to protect personnel, property, and information. When overseas posts identify facilities that do not meet SECCA or OSPB physical security requirements, they first seek ways to bring the facilities into compliance. When this is not possible, the Department may grant the overseas post a waiver, exception, or both. Waivers are requested for deficiencies in the SECCA requirements, and exceptions are requested for deficiencies in the OSPB standards.

The Office of Inspector General (OIG) reviewed the Bureau of Diplomatic Security's (DS) waivers and exceptions processes for physical security deficiencies to determine whether the bureau: (1) developed and implemented internal controls for these processes, (2) ensured the mitigations required by waivers and exceptions were implemented, and (3) identified and addressed organizational, resource, or procedural issues that affected the processes. This review covered the period from January 2018 to December 2023.

Overall, OIG concluded DS implemented some internal controls for the waivers and exceptions processes, which contributed to a reduction in the average processing time from 416 workdays in 2018 to 66 workdays in 2023. The bureau also developed a standard operating procedure, templates, and established timelines and tracking mechanisms. However, OIG found the bureau's tracking mechanisms did not provide the information needed to verify whether its process timelines were being met. Furthermore, OIG determined the bureau did not have formal internal controls in place to ensure mitigations that were approved as part of a waiver or an exception were implemented. Lastly, OIG found DS did not consistently require overseas posts to seek exceptions for facilities that did not meet OSPB standards.

This report includes three recommendations to improve DS' physical security waivers and exceptions processes. In its comments on the draft report, DS concurred with all three recommendations. OIG considers all three recommendations resolved. The bureau's response to each recommendation and OIG's reply can be found in the Recommendations section of this report. The bureau's formal written response is reprinted in its entirety in Appendix B.

BACKGROUND

Security standards are in place to reduce risk and vulnerabilities to facilities under COM authority to protect personnel, property, and information. The Department's security standards address six categories of threat: political violence, human intelligence, technical, crime, indigenous terrorism, and transnational terrorism. The Department assesses threat levels at

least annually as critical, high, medium, and low for each threat category.[1] The standards specify the appropriate countermeasures for the facility type, building category, and level of threat that exists at each overseas post.

When overseas posts identify facilities that do not meet Department security standards, they first seek ways to bring the facilities into compliance with the SECCA requirements[2, 3] or the OSPB[4] standards. When this is not possible, the Department may grant a waiver, exception, or both.[5] Waivers are requested by overseas posts for deficiencies in SECCA's statutory requirements for co-location and setback. Exceptions are requested by overseas posts for deficiencies to the OSPB security standards, which are non-statutory. When requesting a SECCA waiver or OSPB exception, regional security officers (RSO) at overseas posts work with the DS Office of Physical Security Programs' (PSP) Project Coordination Division (PCD),[6] which manages the waivers and exceptions processes, to conduct a formal risk assessment that identifies security deficiencies, documents proposed mitigations, and analyzes the remaining risk. Using this information, Department leadership then determines whether it is possible to meet the standard, whether to spend resources to meet the standard,[7] or whether to grant a waiver or exception to the standard and accept the risk.

[1] According to 12 Foreign Affairs Handbook (FAH)-6 H-511.3b, the level of each of the six threat categories is continually reassessed for each overseas post by the Department. The Department, in consultation with appropriate members of the OSPB, issues on a semiannual basis a Security Environment Threat List (SETL). The SETL determines which standards apply to a particular overseas post.

[2] Under the Secure Embassy Construction and Counterterrorism Act (SECCA) of 1999, Pub.L. 106-113 (Nov. 29, 1999), in selecting a site for any new U.S. diplomatic facility abroad, all U.S. government personnel at the overseas post, except those under the command of an area military commander, must be co-located on the site. Additionally, each newly acquired U.S. diplomatic facility must have a 100-foot setback. See 12 FAH-5 H-311a.

[3] The National Defense Authorization Act for Fiscal Year 2023, Pub.L. 117-263 (2022), included amendments to SECCA, such as allowing the Secretary of State new discretion to determine that personnel occupying particular types of facilities need not be subject to co-location requirements and to determine minimum threat ratings at which facilities at overseas posts would be subject to SECCA requirements in the first instance, and eliminating restrictions on the Secretary's authority to delegate the granting of SECCA waivers.

[4] The Overseas Security Policy Board (OSPB) is an interagency consultative body that assists the Secretary of State in carrying out statutory responsibilities to provide for the security of United States government operations at U.S. missions abroad. The OSPB considers, develops, coordinates, and promotes security policies, standards, and agreements on overseas security operations, programs, and projects that affect all U.S. government agencies under COM authority.

[5] An overseas post may request both a SECCA waiver and an OSPB exception at the same time.

[6] PCD evaluates projects to ensure proper application of physical security standards in the selection, design, construction, and modification of buildings abroad to be occupied by the Department and other agencies. PCD ensures compliance with OSPB (12 FAH-6) and Department security standards (12 Foreign Affairs Manual, 12 FAH-5) and coordinates SECCA waiver and OSPB exception requests when standards cannot be met.

[7] For example, although an overseas post initially might determine it can bring its facility into compliance with physical security standards, DS and the Bureau of Overseas Buildings Operations (OBO) could determine that is not possible from an engineering standpoint or it is too costly to do so and offer alternative steps to mitigate the deficiency as part of a waiver or exception.

Determining When a Waiver or Exception Is Required

The Department's triennial physical security survey[8] is the primary means by which an overseas post identifies facilities that do not meet physical security standards. Any deficiency identified through a physical security survey is entered into the DS physical security deficiency database[9] and the Bureau of Overseas Buildings Operations' (OBO) Building Management Integrated System (BMIS).[10] PCD then works with the overseas post and OBO to determine if it is feasible to bring the facilities with deficiencies into compliance with SECCA requirements and OSPB physical security standards, or if a waiver or exception is required.

The first steps in determining feasibility are to identify the type of facility—such as a chancery, tenant commercial space,[11] or public office facility[12]—and category of building. In terms of physical security for U.S. government facilities abroad, DS defines three categories of buildings: existing office buildings (EOB), newly acquired buildings (NAB), and new office buildings (NOB). DS further defines two types of EOBs: (1) Department-designed office buildings that were at the 35 percent "design development stage" (i.e., where building designs were 35 percent complete) prior to July 1991, and (2) office buildings that were not designed by the Department and that the Department acquired through purchase, lease, or other means, before July 1991.[13] A NAB is an office building not constructed by or on behalf of the U.S. government, which the Department acquired by purchase, lease, or other means, after June 1991.[14] A NOB is an office building, constructed by or on behalf of the U.S. government, which was at the 35 percent design development stage subsequent to June 1991.[15]

[8] At least once every 3 years or upon the acquisition of a new facility, major renovation, or major security upgrade, regional security officers must conduct physical security surveys of their post's facilities to determine if the facilities meet the required standards and, if not, identify deficiencies requiring correction. 12 FAM 315.2, "OSPB Security Standards – Exception Authority."

[9] A DS-maintained system of record for published physical security deficiencies.

[10] BMIS is the OBO central repository for all minor construction and improvement (MCI) requirements. The purpose of BMIS is to maintain a worldwide inventory of MCI requirements for current and future fiscal years, to prioritize those requirements across program offices based on importance and urgency, and to track approved MCI projects from initial funding to project completion.

[11] A commercial office building that is not solely occupied by the U.S. government.

[12] A facility which exists for the use of public functions such as American Centers and commercial offices and is located in a commercial or residential building not co-located on an overseas post's compound. The U.S. government may or may not be the sole occupant of this facility type.

[13] 12 FAH-5 H-041, "Terms/Acronyms." The Department adopted new security-related construction standards in June 1991.

[14] Ibid.

[15] Ibid.

EOBs are not required to have exceptions[16] for physical security deficiencies. If, however, OBO has a major renovation[17] of the facility planned, PCD, in coordination with the overseas post and OBO, will consider physical limitations, legal constraints, and practicality—such as the cost of installing necessary security features—to determine if it is feasible to bring any identified deficiencies into compliance with standards. If it is feasible to do so, the physical security upgrades may become part of the OBO project.

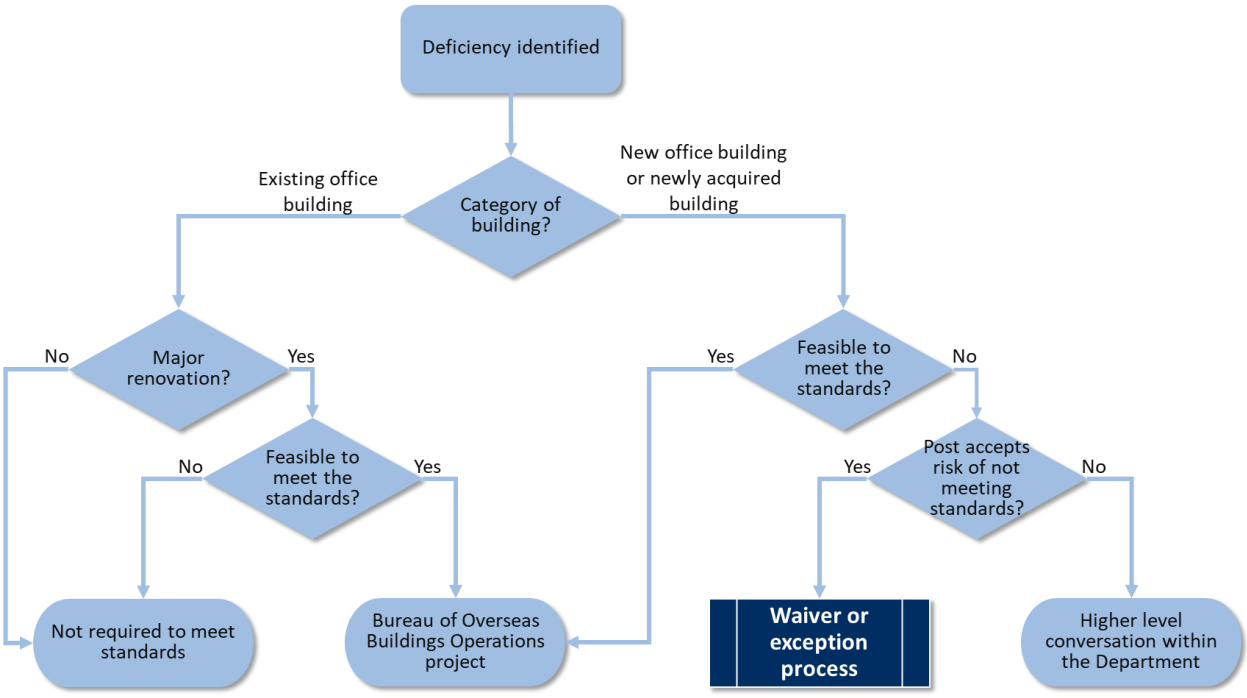
As described above, an EOB is any Department-designed office building that was acquired or leased prior to July 1991. A leased EOB converts to a NAB when a new lease for that building is signed. NABs and NOBs that do not meet physical security standards must have a waiver or exception as applicable.[18] If a NAB or NOB can feasibly be brought into compliance with Department physical security standards, the deficiencies are documented in the physical security deficiency database and BMIS, an interim mitigation plan is implemented, and a future project to upgrade the facility is placed on a rank-ordered list for funding by OBO. If stakeholders determine a facility cannot feasibly be brought into compliance with applicable security standards and an overseas post agrees to accept the risk of not complying with standards, a waiver or exception is required. It is incumbent on an overseas post to request the waiver or exception. (See Figure 1 for a decision tree illustrating when a waiver or exception is required.) The processes for requesting and granting a waiver or exception were the primary focus of this review.

[16] All facilities abroad, constructed or acquired after November 29, 1999, must meet SECCA's setback and co-location requirements, unless the requirements are waived in accordance with established procedures.

[17] Projects executed on an existing facility falling under COM authority for which the work area exceeds 50 percent of the building area.

[18] According to 12 FAH-5 H-122, "New office facility construction (i.e., new office buildings (NOBs) and newly acquired buildings (NABs)), whether acquired by purchase, capital lease or operating lease unless otherwise specified in the standards, must meet all physical security standards. This includes all new construction on occupied property, such as chancery annexes and additions. Diplomatic Security (DS) only grants an exception to this requirement when a persuasive justification indicates it is in the national interest or meeting the standard(s) is not feasible because of physical limitations, legal restraints, or practicality."

Figure 1: Decision Tree: Determining When a Waiver or Exception Is Required



Source: Compiled by OIG from data provided by DS.

Waivers and Exceptions Processes

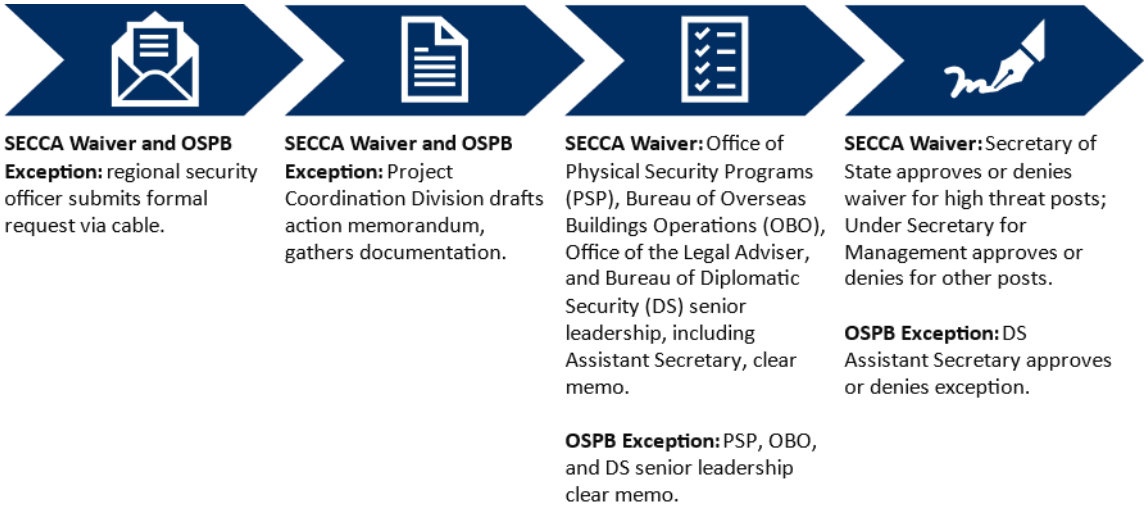
Once it is determined that a waiver or exception is required, PCD assists RSOs at overseas posts in preparing these requests. Overseas posts are required to provide a specific set of information for waivers and exceptions requests, including the standard(s) involved, a justification, a statement of agency operational requirements, proposed steps to mitigate the deficiency, and supporting documentation. Emergency Action Committee[19] and COM concurrences are also required, and the request must be made through a formal, front channel cable to the Department. Once PCD receives an overseas post's cable, it creates a request approval package and coordinates the request approval process. The request approval package includes an action memorandum to the appropriate approving official, the information sent by post to document its request, and a plan for mitigating the identified deficiency.

SECCA waiver and OSPB exception requests follow a similar approval process. PCD ensures all required documentation is present in the request approval package and obtains concurrence for the request from internal DS and external Department stakeholders, including OBO, the regional bureau and the Under Secretary for Management, as necessary. SECCA waivers also require the concurrence of the Office of the Legal Adviser before proceeding to the final

[19] According to 12 FAH-1 H-233.2a, "the Emergency Action Committee collaborates to analyze risk and provide the COM [or principal officer] recommendations on preparing for and responding to emergencies and potential changes in risk that might impact the health, safety and security of a mission, U.S. government personnel and accompanying family members under COM security responsibility, and the private U.S. citizen community."

approval stage. The Secretary of State delegated authority to approve SECCA waivers to the Under Secretary for Management for all embassies and consulates not located in designated high threat environments. The Secretary approves SECCA waivers for embassies and consulates in designated high threat environments. OSPB exception requests are approved by the Assistant Secretary for Diplomatic Security. Figure 2, below, summarizes both processes.

Figure 2: SECCA Waiver and OSPB Exception Request Processes



Source: Compiled by OIG from data provided by DS.

Following the approval of a waiver or exception, DS will send a formal, front channel notification cable to the overseas post. The overseas post, in coordination with OBO, is then responsible for implementing the mitigations that formed part of the approved waiver or exception.

FINDINGS

Internal Controls for the Waivers and Exceptions Processes

OIG reviewed the physical security waivers and exceptions processes for existing Department facilities abroad and found PCD implemented an internal control system that helps the Department document, adjudicate, and process requests. Specifically, DS and PCD:

- Developed an internal standard operating procedure and process maps to document the waivers and exceptions processes.
- Established timeline targets for the overall waivers and exceptions processes, as well as for interim steps such as the time for PCD to draft an action memorandum.
- Implemented a tracker for waivers and exceptions requests.
- Created templates to ensure standard required information and concurrences were included in the requests.

- Established a new position, the Waivers and Exceptions Coordinator, responsible for the overall monitoring and documentation of the processes.

As detailed below, OIG found DS did not have certain information that would enable it to monitor the efficiency of the processes. Despite this, OIG calculated that since 2018, the Department had reduced the average processing time for waivers and exceptions, and determined the Department generally met its process timeline targets.

The Project Coordination Division Lacked Key Tracking Information to Assess the Timeliness of the Waivers and Exceptions Processes

Although PCD had established timeline targets, OIG determined the division lacked information that would enable it to assess the timeliness of the waivers and exceptions processes, for both the overall processes as well as interim steps. Specifically, OIG found:

- The PCD waivers and exceptions tracker did not contain date fields to capture the start and end dates of each step in the clearance processes.
- The PCD tracker did not have a date field to document when a request package was complete (i.e., included all required components). PCD required a complete request package to initiate the clearance process.
- PCD did not have an established timeframe for sending the response cable once the request was approved or denied.
- PCD did not have consistent guidance for how dual requests—requests for both a waiver and an exception, which have different approvals and target timelines—should be entered into the tracker.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, Principle 13.05,[20] states that management uses quality information[21] to evaluate the entity's performance in achieving key objectives. OIG attributed the information gaps to the fact that PCD's internal tracker was designed to track individual requests through the overall process and not as a tool to monitor the efficiency of the processes. However, without more granular data, PCD will not be able to assess compliance with the established timelines for the waivers and exceptions processes or identify and resolve bottlenecks or other potential areas for improvement.

Recommendation 1: The Bureau of Diplomatic Security should modify the waivers and exceptions tracker to provide more granular data to assess compliance with established process timelines and to identify and resolve bottlenecks in the waivers and exceptions processes. (Action: DS)

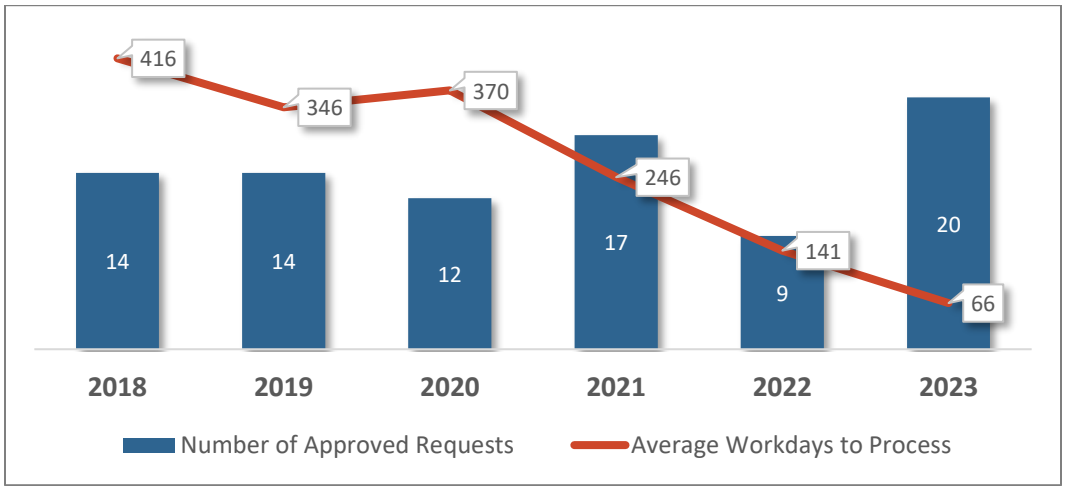
[20] Government Accountability Office, *Standards for Internal Control in the Federal Government*, page 60 (GAO-14-704G, September 2014).

[21] The *Standards for Internal Control in the Federal Government* defines quality information as "appropriate, current, complete, accurate, accessible, and provided on a timely basis." GAO-14-704G, September 2014, page 60.

Department Improved the Overall Processing Time for Approving Waivers and Exceptions, Which Generally Met Established Targets

Despite the lack of information in the PCD tracker, OIG calculated that since 2018, the Department had reduced the average processing time for waivers and exceptions, and determined the Department generally met process timeline targets of 82 workdays for a SECCA waiver and 43 workdays for an OSPB exception.[22] On average, approved requests made in 2018 were processed in 416 workdays, while approved requests initiated in 2023 were processed within 66 workdays, as shown in Figure 3.

Figure 3: Overall Processing Times for Approved Waivers and Exceptions Requests



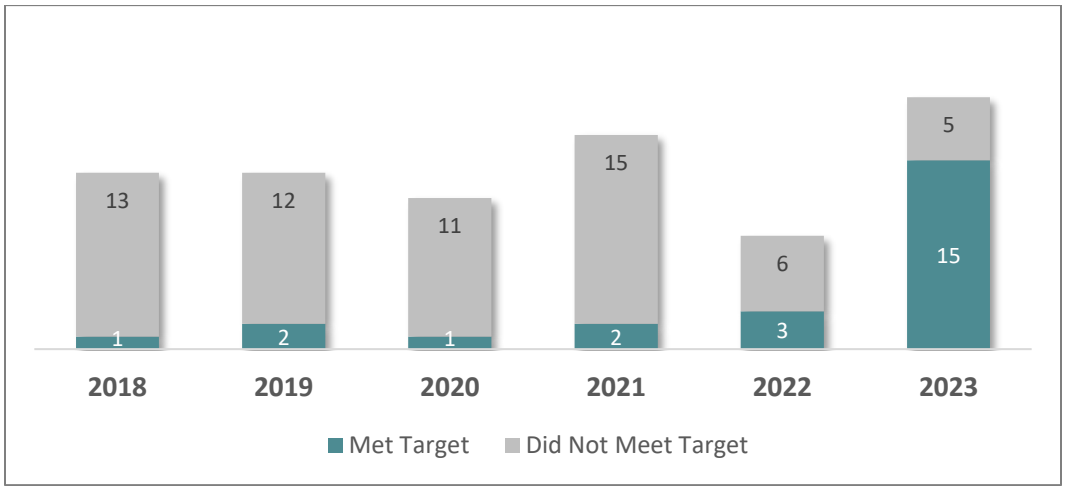
Source: OIG calculations based on data contained in PCD's tracker and Department cables.

Furthermore, as shown in Figure 4, OIG calculated that 75 percent of the requests initiated in 2023 (15 of 20) were processed within the overall targets of 82 workdays for a SECCA waiver and 43 workdays for an OSPB exception. In contrast, in 2018, only 7 percent of requests (1 of 14) were approved within the current targets.[23]

[22] OIG analyzed the overall processing times by reviewing the dates of cables where an embassy requested a waiver, exception, or both, and of cables from DS approving the waiver, exception, or both. OIG calculated the number of workdays from the date of the request cable to the date of the approval cable. OIG limited its calculations to requests that completed the processes, to ensure a start and end date for the calculation.

[23] OIG did not find any processing targets prior to the current targets, which were established in 2022.

Figure 4: Approved Requests That Met Timeline Targets for SECCA Waivers and OSPB Exceptions



Source: OIG calculations based on data contained in PCD's tracker and Department cables.

Internal Controls to Ensure Implementation of Mitigations in Approved Waivers and Exceptions

As described earlier in this report, after an overseas post receives notification that a waiver or exception is approved, it is then responsible for implementing the mitigations that formed part of the approved waiver or exception. PCD defines a mitigation plan as a strategy to counter a potential threat caused by not meeting SECCA or OSPB standards.[24] PCD further defines two types of mitigation plans: interim and permanent mitigation plans. An interim mitigation plan is a short-term solution, implemented until an OBO-funded project is prioritized to remedy the deficiency. After the project is completed, the interim mitigation plan is no longer needed. A permanent mitigation plan is implemented when the Department determines it is not feasible to meet a physical security standard; this type of plan is a key element of waivers and exceptions requests. These mitigation plans must provide countermeasures that logically address the physical security standards that cannot be met.

According to Department cables,[25] responsibility for these mitigation plans rests with RSOs at overseas posts and PCD desk officers. RSOs are charged with ensuring that all deficiencies at overseas post facilities have been identified and for creating the mitigation plans. RSOs must also ensure the appropriate waivers and exceptions are documented, approved by the Department, and that mitigation plans are executed as required by SECCA and OSPB standards.

[24] Although 12 FAH 5 H-200 and 12 FAM 315 do not mention or define the term "mitigation plan," PCD defined the term in training documents for its staff.

[25] Cables 17 STATE 98644 and 19 STATE 122810 describe regional security officer responsibilities for physical security and for identifying physical security deficiencies. Cables 17 STATE 98644, "DS Physical Security Waivers/Exceptions Database (Part I)," September 26, 2017, and 19 STATE 122810, "Department and Mission Responsibilities for Physical Security of Diplomatic Facilities," November 21, 2019.

PCD desk officers then input reported mitigation plans into the PCD mitigation plans database, which PCD uses to track the plans.

OIG reviewed PCD's internal controls and identified an issue with the verification of the mitigation plans as detailed below.

Department Did Not Have Formal Internal Controls to Verify Implementation of Mitigations as Part of Approved Waivers and Exceptions

As noted earlier in this report, PCD implemented an internal control system to document, adjudicate, and process waivers and exceptions requests. However, OIG determined PCD lacked formal internal controls to verify the final step in the processes: the implementation of mitigation plans required as part of the approved waivers or exceptions packages. Specifically, PCD did not have a formal internal control system that described when mitigations were implemented, where this information was documented, or who was responsible for verifying the information.

Cable 19 STATE 122810 states RSOs must report the completion of mitigation plans to PCD. However, the cable does not provide specific guidance on who is responsible for verifying that mitigations were completed and implemented. Furthermore, OIG reviewed PCD's standard operating procedures and found they did not include information on mitigations.

Additionally, in interviews with OIG, PCD desk officers confirmed there was no formal verification process to ensure that mitigations were implemented. Although PCD tracked mitigations in the mitigation plans database, staff members told OIG that the only way they know if a mitigation was implemented is if the RSO reports the information to them, or if someone from PCD visits the overseas post and observes that the mitigation was implemented. Some desk officers told OIG they conducted their own verification to ensure mitigations were implemented, including conducting an annual "score card" review with RSOs, where they reviewed mitigations. PCD staff also described a past practice—last completed prior to the COVID-19 pandemic and under previous PCD leadership—where the division annually reviewed with RSOs all mitigations for their overseas posts. Staff acknowledged to OIG that due diligence, communication, and coordination among desk officers, RSOs, and OBO is needed to ensure mitigations are implemented.

In accordance with the GAO *Standards for Internal Control in the Federal Government*, OV2.16-20 and Principles 10.03, 12.01-12.05 and 14.01-14.03, organizations should have internal control systems in place to carry out the objectives and duties of an entity efficiently, design the appropriate type of control activities, implement and review those control activities, and effectively communicate throughout the organization. Failure to verify that overseas posts have implemented mitigations required by approved waivers and exceptions could result in those mitigations being overlooked, risking the security of Department facilities.

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, should implement internal controls to verify whether all

aspects of each mitigation plan are fully implemented, as required by the approved waivers and exceptions packages. (Action: DS, in coordination with OBO)

Organizational, Resource, and Procedural Issues That Affected the Waivers and Exceptions Processes

In determining whether PCD had identified and addressed organizational, resource, or procedural issues that have affected the physical security waivers and exceptions processes, OIG identified an issue with the inconsistent application of Department standards requiring overseas posts to obtain OSPB exceptions, as described below.

The Project Coordination Division Did Not Consistently Apply Department Standards Requiring Overseas Posts to Obtain Exceptions for Physical Security Deficiencies

OIG found PCD did not consistently apply Department standards requiring overseas posts to seek exceptions for facilities that do not meet OSPB standards. According to 12 Foreign Affairs Manual (FAM) 315.2, all new facilities must meet all OSPB security standards, whether constructed or acquired by purchase or lease. If compliance with one or more OSPB standards is not possible for a specific facility, the overseas post must apply for an exception.[26]

In 2019, DS issued cable guidance[27] describing the responsibilities for COMs and deputy chiefs of mission to ensure overseas posts review physical security at diplomatic facilities and mitigate and document deficiencies where necessary. The cable also reinforced the 12 FAM 315.2 requirements, stating that when a facility cannot comply with standards, the COM, in coordination with the RSO and the Emergency Action Committee, must submit a cable citing the deficiencies, describe the proposed mitigations, and request a waiver or exception for the Department's approval.

However, OIG found there were some overseas posts with documented physical security deficiencies that did not have approved exceptions. Specifically, through a review of seven OIG inspection reports since 2015,[28] OIG identified at least 14 recommendations regarding physical security deficiencies at different overseas posts.[29] Yet, OIG was unable to locate the approved exceptions for any of these documented deficiencies in the appropriate DS databases.[30] When OIG discussed this matter with PCD staff, they told OIG that once a deficiency has been documented in the DS physical security deficiency database, it means that OBO has

[26] As noted previously in this report, exception requests are not required for EOBs.

[27] Cable 19 STATE 122810, "Department and Mission Responsibilities for Physical Security of Diplomatic Facilities," November 21, 2019.

[28] As the reports are classified and the recommendations pertain to physical security vulnerabilities, OIG is not including the titles of the inspection reports.

[29] The overseas posts included two from the Bureau of African Affairs, one from the Bureau of East Asian and Pacific Affairs, two from the Bureau of European and Eurasian Affairs, and two from the Bureau of Near Eastern Affairs.

[30] OIG reviewed the following DS databases: the waivers/exceptions database, the physical security deficiency database, and the physical security surveys database.

acknowledged the deficiency, and the deficiency will be addressed in a future physical security upgrade project or through the construction of a new diplomatic facility. In these instances, PCD staff said that it is at the discretion of the post whether to seek an exception prior to the completion of the physical security upgrade project or the new diplomatic facility.

OIG notes, however, that the FAM and cable guidance described above do not differentiate between physical security deficiencies requiring exceptions and those deficiencies that do not require exceptions because they could be addressed in future physical security upgrade projects or through the construction of a new diplomatic facility. Furthermore, the guidance does not say that posts have discretion about when to seek an exception. Because there is a disconnect between the written guidance and PCD's characterization that posts have discretion to not seek an exception to physical security standards, the Department cannot be assured that it has all the information it needs and is taking all practical steps to ensure the security of overseas diplomatic facilities.

Recommendation 3: The Bureau of Diplomatic Security should update and implement its guidance related to facilities that do not meet Overseas Security Policy Board standards to clearly delineate when exceptions to physical security standards are required and when they are not and ensure that the guidance is consistent with Overseas Security Policy Board standards. (Action: DS)

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. The bureau's complete responses can be found in Appendix B.

Recommendation 1: The Bureau of Diplomatic Security should modify the waivers and exceptions tracker to provide more granular data to assess compliance with established process timelines and to identify and resolve bottlenecks in the waivers and exceptions processes. (Action: DS)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Security concurred with this recommendation. The bureau noted that it modified the waivers and exceptions tracker to include dates for each equity's tasking and when each clearance is completed, fostering added transparency, accountability, flexibility, and operational efficiency. The bureau requested the recommendation be closed.

OIG Reply: OIG considers the recommendation resolved. During compliance, OIG will review the modified waivers and exceptions tracker documentation and will close the recommendation upon determination that the modifications provide more granular data to assess compliance with established process timelines and to identify and resolve bottlenecks in the waivers and exceptions processes.

Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, should implement internal controls to verify whether all aspects of each mitigation plan are fully implemented, as required by the approved waivers and exceptions packages. (Action: DS, in coordination with OBO)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Security concurred with this recommendation. The bureau noted an estimated completion date of January 1, 2025.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Diplomatic Security implemented internal controls to verify whether all aspects of each mitigation plan are fully implemented, as required by the approved waivers and exceptions packages.

Recommendation 3: The Bureau of Diplomatic Security should update and implement its guidance related to facilities that do not meet Overseas Security Policy Board standards to clearly delineate when exceptions to physical security standards are required and when they are not and ensure that the guidance is consistent with Overseas Security Policy Board standards. (Action: DS)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Security 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 Diplomatic Security updated and implemented its guidance related to facilities that do not meet Overseas Security Policy Board standards to clearly delineate when exceptions to physical security standards are required and when they are not and ensured that the guidance was consistent with Overseas Security Policy Board standards.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This review was conducted from January 2 to March 15, 2024, 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).

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 review were to determine whether the Bureau of Diplomatic Security has:

1. Developed and implemented internal controls for the physical security waivers and exceptions process that promote effective and efficient operations and ensure compliance with applicable laws and regulations.
2. Developed and implemented internal controls to ensure that mitigations required by waivers or exceptions have been implemented.
3. Identified and addressed organizational, resource, or procedural issues that have affected the physical security waivers and exceptions process.

The scope for this review was all physical security waivers and exceptions requested by overseas posts from January 1, 2018, through December 31, 2023.

OIG used a risk-based approach to prepare for this review. OIG conducted portions of the review remotely and relied on audio- and video-conferencing tools in addition to in-person interviews with Department and other personnel. OIG also reviewed pertinent records; circulated surveys and compiled the results; and discussed 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.

Marlene Abshire (Team Leader), Kristi Hogan (Co-Team Manager), Lisa Derrickson (Co-Team Manager), and Hanane Grini conducted this review. Other report contributors included Dolores Adams and Rebecca Sawyer.

APPENDIX B: MANAGEMENT RESPONSE

United States Department of State

Washington, DC 20520

UNCLASSIFIED

May 28, 2024

☐ Read by _____

Info Memo for Acting Inspector General Arne Baker – OIG

FROM: DS – Gentry O. Smith

SUBJECT: Bureau of Diplomatic Security's Response to the Draft Report Review of the Bureau of Diplomatic Security's Physical Security Waivers and Exceptions Processes (ISP-I-24-19)

Below is the Bureau of Diplomatic Security's response to OIG's draft report, including Recommendations 1, 2, and 3.

DS Response to Audit Findings and Recommendations:

DS has remained resolutely committed to the rigorous enforcement of the 12 FAH-6 Overseas Security Policy Board (OSPB) security standards. In coordination with the Bureau of Overseas Buildings Operations (OBO), DS ensures seamless integration of security considerations throughout the planning and execution phases of diplomatic facility projects. Such proactive collaboration includes formally chartered committees, the Security Standards Committee and High Threat Posts Security Requirements Working Group, along with the Compound Security Upgrade Working Group and other intra-bureau and stakeholder engagement. These meetings, often convening weekly, focus expertise and available resources on timely resolution of issues to ensure that the Department facilities meet requisite security standards.

DS has taken proactive steps to enhance physical security training courses for its desk officers, both new and seasoned. These courses comprehensively cover the proper implementation of 12 FAH-6 OSPB

UNCLASSIFIED

requirements, ensuring that its staff is properly equipped to navigate and enforce security standards and requirements effectively.

Additionally, DS remains committed to providing Regional Security Officers (RSOs) with comprehensive and in-depth tools to conduct thorough physical security surveys. To this end, DS is preparing to launch a reimagined version of the physical security survey application in June 2024. The updated application will provide RSOs with enhanced capabilities to conduct detailed reviews of posts' physical security, facilitating a more comprehensive assessment and ensuring alignment with the 12 FAH-6 OSPB standards.

Draft Recommendation 1: The Bureau of Diplomatic Security should modify the waivers and exceptions tracker to provide more granular data to assess compliance with established process timelines and to identify and resolve bottlenecks in the waivers and exceptions processes. (Action: DS)

DS Response (5/28/2024): DS concurs with the OIG's recommendation. Since the closure of the OIG's audit, the Office of Physical Security Program's Project Coordination Division (DS/PSP/PCD) has modified the waivers and exceptions (W/E) tracker to provide more granular data to assess compliance with established process timelines and to identify and resolve bottlenecks in the waivers and exceptions processes. Specifically, the W/E tracker now includes dates for each equity's tasking and when each clearance is completed, fostering added transparency, accountability, flexibility, and operational efficiency (see Tab 1). DS requests that this recommendation be closed.

Draft Recommendation 2: The Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, should implement internal controls to verify whether all aspects of each mitigation plan are fully implemented, as required by the approved waivers and exceptions packages. (Action: DS, in coordination with OBO)

DS Response (5/28/2024): DS concurs with this recommendation. Some internal controls that are implemented to verify mitigation plans are

dependent on coordinated efforts across the entire Department – not exclusively DS or OBO. By January 1, 2025, DS, with consultation from OBO, will establish a quality control process to ensure mitigation plans contained within W/Es are tracked and implemented.

Draft Recommendation 3: The Bureau of Diplomatic Security should update and implement its guidance related to facilities that do not meet Overseas Security Policy Board standards to clearly delineate when exceptions to physical security standards are required and when they are not and ensure that the guidance is consistent with Overseas Security Policy Board standards. (Action: DS)

DS Response (5/28/2024): DS concurs with this recommendation. 12 FAM 310, 12 FAH-5 H-120, and 12 FAH-5 H-210 guidance is subject to recurring, periodic review. By December 1, 2024, DS will target these specific subchapters for review to clarify guidance related to facilities that do not meet Overseas Security Policy Board (OSPB) standards to clearly delineate when exceptions to physical security standards are required and when they are not, ensuring that the updated guidance is consistent with OSPB standards.

Attachment

Tab 1 – Recommendation 1: W/E Tracker Date Fields

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