Office of Inspector General
United States Department of State

AUD-SI-21-04 | Office of Audits | December 2020

(U) Management Assistance Report: The Bureau of Diplomatic Security's Compliance Process Related to Post Security Program Reviews Needs Improvement

MANAGEMENT ASSISTANCE REPORT

(U) CONTENTS

(U) BACKGROUND 2
(U) The Post Security Program Review Process 2
(U) The Post Security Program Review Compliance Process 3
(U) Purpose of the Management Assistance Report 3
(U) RESULTS 4
(U) Finding A: PSPR Compliance Process Needs Improvement 4
(U) RECOMMENDATIONS 14
(U) APPENDIX A: BUREAU OF DIPLOMATIC SECURITY RESPONSE 15
(U) OIG AUDIT TEAM MEMBERS 18

(U) Summary of Review

(U) The Bureau of Diplomatic Security (DS) is the Federal law enforcement and security bureau of the Department of State (Department) and has the largest global reach of any U.S. Federal law enforcement agency. DS has 253 regional security offices led by a U.S. direct-hire regional security officer (RSO) with oversight responsibility for more than 280 locations around the world. One method DS uses to oversee the regional security offices located at overseas posts is the Post Security Program Review (PSPR) program. The High Threat Programs Directorate (HTP) within DS conducts PSPRs for high-threat, high-risk (HTHR) posts. A PSPR consists of consultations with relevant DS offices, document reviews, observations at post, and interviews with post personnel to evaluate a regional security office's level of compliance with selected requirements on topics such as life safety and emergency preparedness.[1] The PSPR team documents noncompliant areas and makes recommendations to address these areas in a PSPR report sent to the post's deputy chief of mission and RSO. The RSO must respond to recommendations with a corrective action plan,[2] and HTP officials must work with RSOs to ensure that corrective action has been taken at post for each noncompliant item.[3]

(U) During an audit of the PSPR program, the Office of Inspector General (OIG) found that although DS has designed a compliance process to assess posts' resolution of recommendations made to address security deficiencies, the PSPR compliance process needs improvement. For example, OIG found that HTP officials did not always maintain documentation describing corrective actions taken by RSOs in response to PSPR recommendations. Specifically, of 146 PSPR recommendations made to HTHR posts that underwent a PSPR in FY 2018 and FY 2019, HTP officials could not provide OIG with RSO compliance responses for 29 (20 percent) of the recommendations. An HTP official stated that the missing responses were likely due to posts' responses not being properly archived to the PSPR SharePoint site. OIG also found that RSOs did not always provide compliance responses within the required 45 days. Specifically, 13 of 20 (65 percent) compliance responses were untimely and ranged from 17 to 204 days late. This occurred, in part, because neither the Foreign Affairs Manual (FAM), nor the PSPR Standard Operating Procedures (SOP),[4] requires HTP officials to escalate untimely compliance responses to deputy chiefs of mission. Furthermore, OIG found that HTP officials did not always track when compliance responses were due or have a formal process in place to follow up on overdue responses. OIG also found instances of insufficient compliance responses. Specifically, of 117 documented RSO compliance responses to PSPR recommendations made between FY 2018 and FY 2019, OIG determined that 12 (10 percent) were insufficient to comply with requirements set forth in the PSPR SOP, which requires that the RSO outline a plan to resolve noncompliant areas of review. Insufficient responses occurred, in part, because HTP officials did not require

[1] (U) 12 FAM 413.2(a), "Preparation – PSPR Pre-Deployment Review," and 12 FAM 413.3, "Conducting a PSPR."

[2] ~~(SBU)~~ Department memorandum, "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) – For Internal Staff Use," January 17, 2020.

[3] (U) 12 FAM 413.4(d), "PSPR Completion."

[4] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

evidence or supporting documentation that demonstrates RSOs have fully implemented recommendations. As a result, HTP officials closed PSPR recommendations that were not fully addressed and were repeated in subsequent PSPR reports.

(U) Until these weaknesses with the PSPR compliance process are addressed, DS will have limited assurance that security deficiencies identified during PSPRs at HTHR posts, which are inherently at higher risk due to continuous security threats, have been remediated as recommended. Therefore, OIG made three recommendations to DS that are intended to improve the PSPR compliance process. In response to a draft of this report, DS concurred with the recommendations offered. On the basis of DS's concurrence with the recommendations and planned actions, OIG considers the three recommendations resolved, pending further action. A synopsis of DS's response to the recommendations offered and OIG's reply follow each recommendation in the Results section of this report. DS's response to a draft of this report is reprinted in its entirety in Appendix A.

(U) BACKGROUND

(U) The Post Security Program Review Process

(U) DS is the Federal law enforcement and security bureau of the Department and has the largest global reach of any U.S. Federal law enforcement agency. DS has 253 regional security offices led by a U.S. direct-hire regional security officer with oversight responsibility for more than 280 locations around the world. According to DS officials, DS created the PSPR program in 2008 as a mechanism to oversee the regional security offices located at overseas posts. The goal of the PSPR program is to "ensure that posts competently manage life safety, emergency preparedness, and information security programs with full mission support and participation, sufficient resources, and appropriate management controls."[5] Embassies, consulates general, and consulates are the main types of posts reviewed.[6]

~~(SBU)~~ HTP conducts PSPRs for HTHR posts.[7] In 2019, 36 HTHR posts were under HTP's purview, 27 of which were required to undergo a PSPR per the PSPR SOP.[8] A PSPR is designed to evaluate a regional security office's level of compliance with selected requirements[9] in several areas, listed in the PSPR Compliance Rating Form:[10]

[5] (U) 12 FAM 413.1, "Overview."

[6] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

[7] (U) 12 FAM 413.1-1(a), "PSPR Frequency."

[8] (U) DS's International Programs Directorate also conducts PSPRs for non-HTHR posts, including annual PSPRs for two posts. For this Management Assistance Report, OIG only reviewed PSPRs conducted at HTHR posts.

[9] (U) 12 FAM 413.3(a).

[10] (U) The PSPR Compliance Rating Form lists selected life safety, emergency preparedness, and other security programs. PSPR program review officers must use the form to rate a post's compliance to security standards for the identified security programs.

- Security Directives and Policies
- Life Safety
- Emergency Preparedness
- Safeguarding Classified Material
- Investigations
- Management Requirements
- Reporting Requirements

(U) On the basis of a review of PSPR reports, a PSPR team is composed of at least two program review officers or one or more program review officers and a regional director or deputy regional director.[11] During a PSPR, the team conducts consultations with relevant DS offices and reviews post documentation before traveling to a post. At post, the team reviews documentation, inspects facilities and residences, observes post operations, and interviews post personnel. At the conclusion of the PSPR, the team discusses any noncompliant areas of review with the RSO. The team then documents any best practices identified at the post, any noncompliant areas of review, and any recommendations in a PSPR report sent to the post's deputy chief of mission and RSO.[12]

(U) The Post Security Program Review Compliance Process

(U) In response to a PSPR report, the RSO must upload a response memorandum to the PSPR SharePoint site within 45 days of the PSPR report date. The response must outline the RSO's plan to resolve noncompliant areas of review.[13] According to the FAM, program review officers should work with their respective RSOs to ensure that corrective action has been taken at post for each non-compliant item. If corrective action has been taken, the program review officer should close the recommendation.[14]

(U) Purpose of the Management Assistance Report

(U) This Management Assistance Report is intended to provide communication of deficiencies that OIG identified during an audit of the PSPR program. The objective of the audit was to determine whether DS's PSPR process is sufficient to identify and resolve deficiencies in the management of selected posts' life safety, emergency preparedness, and information security programs. OIG is reporting the deficiencies discussed in this Management Assistance Report in accordance with generally accepted government auditing standards. In performing the work related to these deficiencies, OIG interviewed DS officials, reviewed applicable criteria, and reviewed historical PSPR data and other supporting documentation. OIG believes that the evidence obtained provides a reasonable basis for the conclusions presented in this report.

[11] (U) Regional Directors are responsible for ensuring that security programs implemented at posts are in compliance with Department policies.

[12] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

[13] (U) Ibid.

[14] (U) 12 FAM 413.4(d).

(U) RESULTS

(U) Finding A: PSPR Compliance Process Needs Improvement

(U) OIG found that, although DS has designed a PSPR compliance process to assess posts' resolution of recommendations made to address security deficiencies, the process needs improvement. Specifically, OIG found that HTP officials did not always maintain documentation describing corrective actions as required. An HTP official stated that the missing documentation was likely due to responses not being properly archived to the PSPR SharePoint site. OIG also found that RSOs did not always provide timely compliance responses, in part, because neither the FAM, nor the PSPR SOP, require HTP officials to escalate untimely compliance responses to deputy chiefs of mission. Furthermore, OIG found that HTP officials did not always track when RSO compliance responses were due or have a formal process in place to follow up on overdue compliance responses. OIG also found instances of insufficient compliance responses, which occurred, in part, because HTP officials did not require evidence or supporting documentation that demonstrates the RSOs have fully implemented recommendations. As a result, HTP officials closed PSPR recommendations that were not fully addressed and were repeated in subsequent PSPR reports.

(U) Until these weaknesses with the PSPR compliance process are addressed, HTP will have limited assurance that security deficiencies identified at HTHR posts, which are inherently at higher risk due to continuous security threats, have been remediated as recommended.

(U) HTP Officials Did Not Always Maintain Documentation on Corrective Actions

(U) The PSPR SOP states, "Within 45 days of the PSPR trip report date: The RSO must upload a RSO Response Memo[15] to the PSPR site…"[16] OIG found that HTP officials did not always maintain RSO compliance responses. Specifically, of 146 recommendations made to HTHR posts that underwent a PSPR in FY 2018 and FY 2019, HTP officials could not provide OIG with compliance responses for 29 (20 percent) recommendations.

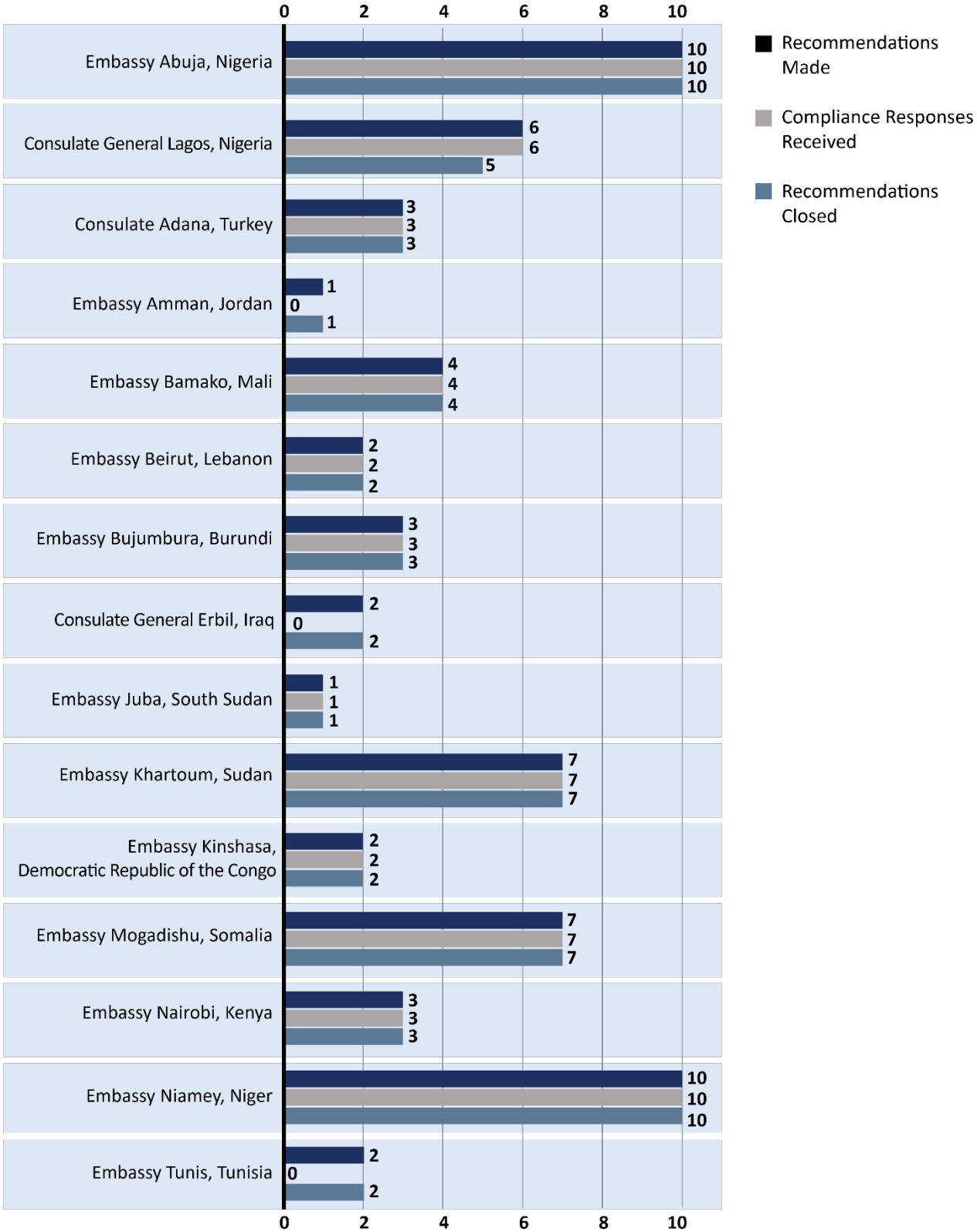
(U) OIG found that 15 HTHR posts that underwent PSPRs in FY 2018 received 63 recommendations. However, HTP officials were unable to provide documentation on corrective actions for five (8 percent) recommendations. These recommendations included updating personnel recovery plans, requesting physical security waivers, and improving the surveillance detection program at post. Figure 1 illustrates the number of FY 2018 recommendations made to HTHR posts, the number of recommendations with a compliance response, and the number of recommendations that have been closed, as of February 2020.[17]

[15] (U) The RSO Response Memo is a compliance response that outlines the RSO's plan to resolve areas of review rated as not compliant.

[16] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

[17] (U) OIG selected February 2020 as the end of the scope period because the audit began in March 2020.

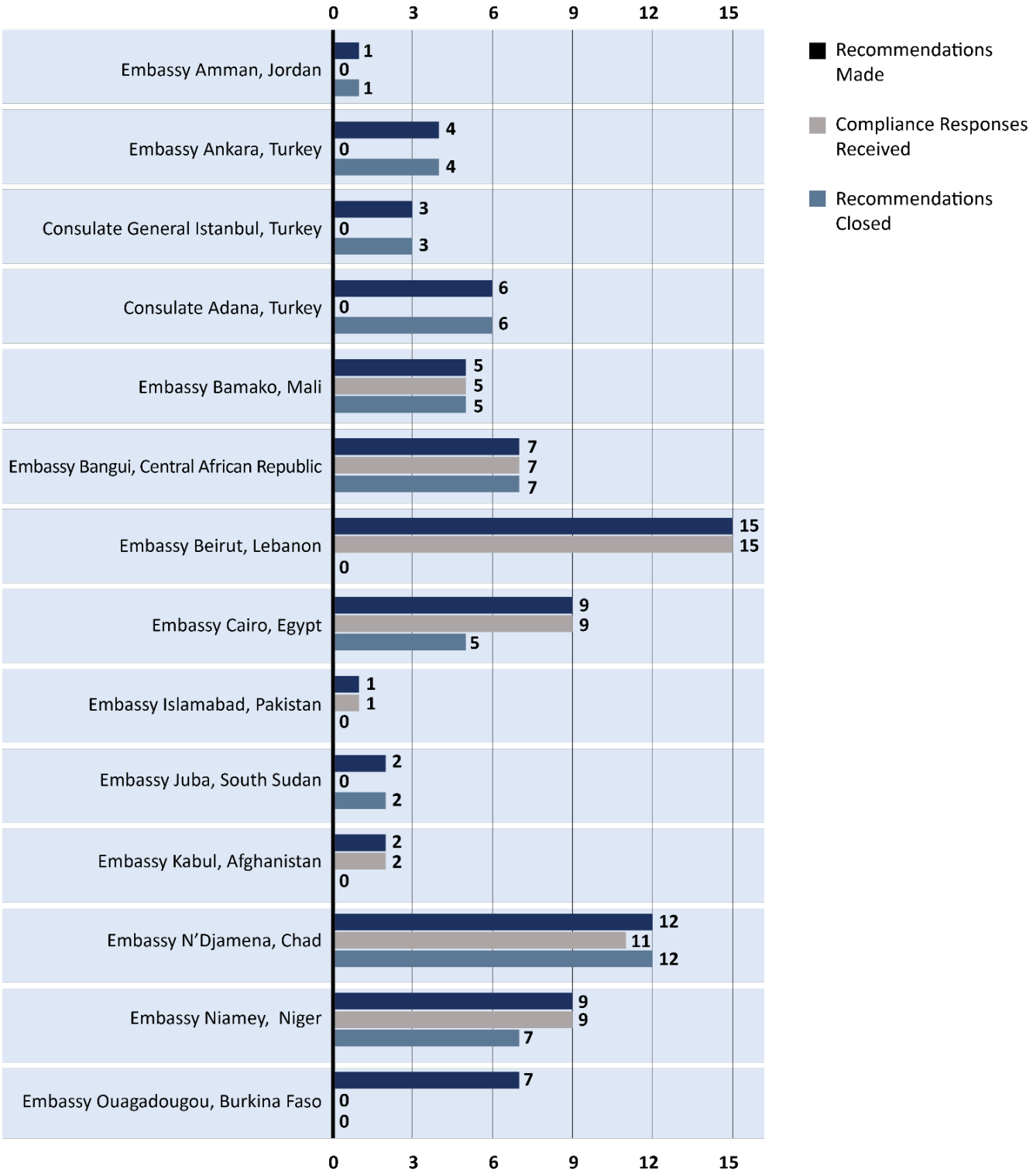
~~(SBU)~~ Figure 1: Number of FY 2018 PSPR Recommendations Made to HTHR Posts, RSO Compliance Responses Received, and Recommendations Closed, as of February 2020



(U) Source: OIG generated based on analysis of PSPR data provided by HTP for FY 2018 as of February 2020.

(U) OIG found that 14 HTHR posts that underwent PSPRs in FY 2019 received 83 recommendations. However, HTP officials were unable to provide documentation on corrective actions for 24 (29 percent) recommendations. These recommendations included updating emergency action plans, installing residential security alarms, and improving the management of the local guard force program. Figure 2 illustrates the number of FY 2019 recommendations made to HTHR posts, the number of recommendations with a compliance response, and the number of recommendations that have been closed, as of February 2020.

~~(SBU)~~ Figure 2: Number of FY 2019 PSPR Recommendations Made to HTHR Posts, RSO Compliance Responses Received, and Recommendations Closed, as of February 2020



(U) Source: OIG generated based on analysis of PSPR data provided by HTP for FY 2019 as of February 2020.

(U) With respect to the missing RSO compliance responses, an HTP official stated that it is likely that they were not properly archived to the PSPR SharePoint site. The HTP official also stated that a majority of PSPR data, including PSPR reports and RSO compliance responses, are manually uploaded to SharePoint, which HTP recognized as a shortcoming. To address the limitation, in July 2020, DS launched a cloud-based application within the "RSO Tools" portal that will automate PSPR processes. According to the official, the application will track all stages of the PSPR process—from scheduling to recommendation compliance. The system will send email notifications to remind RSOs of upcoming deadlines and flag overdue compliance responses. The system will also prompt users to enter status updates for open recommendations every 60 days.

(U) As a result of not always properly archiving RSO compliance responses to the PSPR SharePoint site, HTP officials had limited assurance that HTHR posts resolved the security deficiencies identified during PSPRs. According to HTP officials, the new application within the "RSO Tools" portal will remedy the deficiencies noted above. Because of its recent launch, the new application has not been included in the latest version of 12 FAM 410, "Post Security Programs Oversight" (effective July 23, 2020). Thus, OIG offers the following recommendation.

> **Recommendation 1:** (U) OIG recommends that the Bureau of Diplomatic Security revise Post Security Program Review policies and standard operating procedures to include how the new application within the "RSO Tools" portal has been employed to track regional security officer compliance responses.
>
> **(U) Management Response:** DS concurred with this recommendation, stating that it will revise PSPR policies and SOPs to include how the new application has been employed to track RSO compliance responses.
>
> **(U) OIG Reply:** On the basis of DS's concurrence with the recommendation and planned actions, OIG considers this recommendation resolved, pending further action. The recommendation will be closed when OIG receives and accepts documentation demonstrating that DS has revised the PSPR policies and SOPs to include how the new application has been employed to track RSO compliance responses.

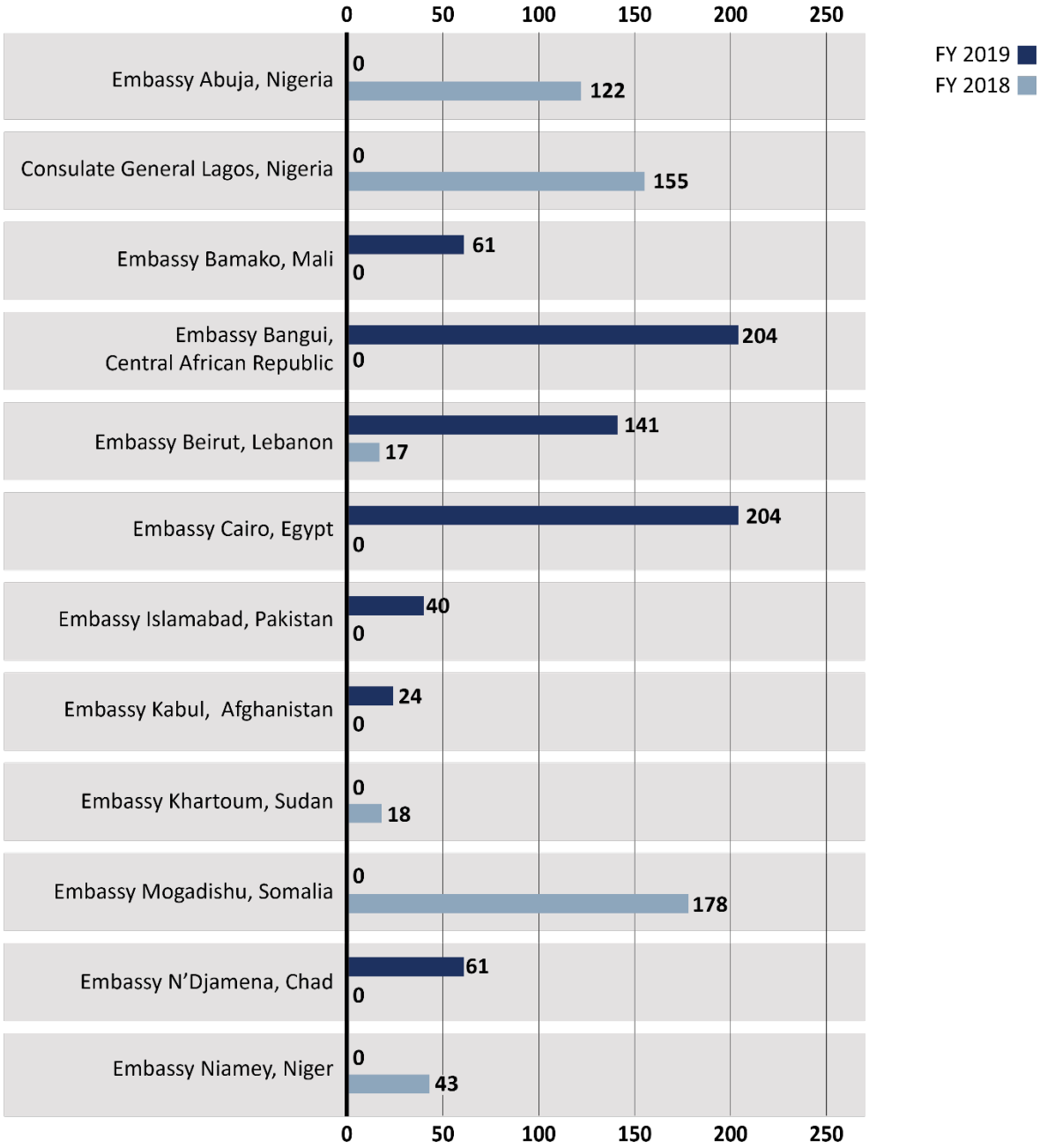
(U) RSOs Did Not Always Provide Timely Responses to PSPR Recommendations

(U) The PSPR SOP states, "Within 45 days of the PSPR trip report date: The RSO must upload a RSO Response Memo to the PSPR site."[18] OIG found that RSOs did not always provide compliance responses to PSPR recommendations within the established 45-day timeframe. Specifically, of the 12 RSOs that provided PSPR compliance responses in FY 2018, 6 (50 percent) did not submit the response within the required 45 days. Of the 8 RSOs that provided PSPR compliance responses in FY 2019, 7 (88 percent) did not submit the response within the required 45 days. Overall, untimely compliance responses ranged from 17 to 204 days late.

[18] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

Figure 3 illustrates the posts that provided untimely compliance responses and the number of days past the 45-day requirement, as of April 2020.

~~(SBU)~~ Figure 3: Number of Days the RSO Response Memo Exceeded the 45-Day Requirement, FYs 2018 and 2019, as of April 2020



(U) Source: OIG generated based on analysis of PSPR reports and RSO compliance responses provided by HTP officials between FY 2018 and 2019, as of April 2020.

(U) The FAM states that program review officers should work with their respective RSOs to ensure that corrective action has been taken at post for each non-compliant item.[19] HTP officials provided various reasons why the 13 RSO responses were untimely, such as RSO staff departures (i.e., "summer turnovers"), temporary duty deployments, and holiday leave. According to HTP officials, program review officers and Regional Directors work with RSOs and, if necessary, higher level officials at posts to address recommendations. However, officials in the PSPR working group[20] stated that "lack of enforcement" is a programmatic concern. Due to the RSO's reporting structure (i.e., they report to a deputy chief of mission), HTP officials cannot penalize RSOs who do not respond to PSPR recommendations in a timely manner. OIG also found that neither the FAM, nor the PSPR SOP, require HTP officials to escalate untimely responses to deputy chiefs of mission. Including this step in PSPR policy and procedures would highlight the importance of providing timely responses.

~~(SBU)~~ OIG also found that HTP officials did not always track when RSO responses were due or have a formal process in place to follow up on overdue responses. For example, Embassy Juba provided a response to the March 2019 PSPR in July 2020—424 days after the required 45-day timeframe.[21] The RSO response stated, "The final version of the PSPR was sent to RSO Juba on April 1, 2019. In July 2020, [HTP] followed up with RSO Juba to capture this RSO response PSPR memorandum. The late submittal of this memorandum falls on [HTP], and not RSO Juba." An HTP official explained that the RSO's response and HTP's follow up efforts were untimely because of staff turnover in HTP and Embassy Juba's Regional Security Office. According to HTP officials, the implementation of the new application within the "RSO Tools" portal will better track RSO compliance responses.

(U) As a result of untimely compliance responses, DS had limited assurance that HTHR posts resolved security deficiencies in a timely manner. Because of the security threats inherent to HTHR posts, more needs to be done to increase DS's assurance that the security deficiencies identified by PSPRs are resolved in a timely manner. OIG is, therefore, offering the following recommendation.

Recommendation 2: (U) OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to clarify requirements for following up on overdue responses from posts related to security deficiencies identified. The update should, at a minimum, include a process for notifying higher level post officials when responses are overdue, a process for tracking when responses are due, and a set schedule (with established intervals and milestones) for following up with posts.

(U) Management Response: DS concurred with the recommendation.

[19] (U) 12 FAM 413.4(d).

[20] (U) The PSPR working group, which is comprised of HTP and International Programs Directorate representatives, meets on an ad hoc basis to recommend changes to the PSPR process.

[21] (U) OIG completed its analyses using data up to April 2020. Thus, OIG included Embassy Juba under the "no response" finding (see Figure 2). HTP provided the Embassy Juba response to OIG in August 2020.

(U) OIG Reply: On the basis of DS's concurrence with the recommendation, OIG considers this recommendation resolved, pending further action. The recommendation will be closed when OIG receives and accepts documentation demonstrating that DS has updated its PSPR policies and SOPs to clarify requirements for following up on overdue responses from posts related to security deficiencies identified. The update should, at a minimum, include a process for notifying higher level post officials when responses are overdue, a process for tracking when responses are due, and a set schedule (with established intervals and milestones) for following up with posts.

(U) RSOs Did Not Always Provide Sufficient Responses to PSPR Recommendations

~~(SBU)~~ The PSPR SOP states, "The RSO must upload a RSO Response Memo to the PSPR site . . . The memo must outline the RSO's plan to resolve areas of review rated as not compliant."[22] OIG found that RSOs did not always provide sufficient responses to PSPR recommendations. Specifically, of 58 RSO compliance responses to FY 2018 recommendations, OIG determined that compliance responses to 10 (17 percent) were insufficient. In addition, of 59 RSO compliance responses to FY 2019 recommendations, OIG determined that the responses to 2 (3 percent) were insufficient. For example, the RSO for Embassy Abuja responded to five FY 2018 recommendations stating only "Compliant." This response is insufficient because it did not comply with the requirement set forth in the SOP to outline a plan to resolve deficiencies, nor did it explain the actions taken to address the recommendations.[23] In another example, HTP recommended to Embassy Niamey that the "RSO must ensure all [local guard force] binders contain current General and post Specific Guard Orders in both English and French. Review all other old notices and emails in order to determine if they remain valid or should be removed." The RSO responded: "Post ensured that all obsolete and outdated materials were removed from the binders located at each Local Guard Force post." This compliance response is insufficient because it only addressed one portion of the recommendation.[24]

[22] (U) "Standard Operating Procedures (SOP) for Post Security Program Reviews (PSPRs) - For Internal Staff Use," January 17, 2020.

[23] ~~(SBU)~~ HTP officials followed up on this response with post and requested information on what had been done to comply with the recommendation. The RSO responded but did not detail specific corrective actions. Although the RSO did not provide details, HTP closed the five recommendations.

[24] ~~(SBU)~~ HTP officials stated that they confirmed that corrective action had been taken during the next PSPR at Embassy Niamey.

(U) One reason for the insufficient compliance responses is that some HTP officials do not require evidence or supporting documentation from posts to close recommendations. Specifically, neither the FAM nor the PSPR SOP require that RSOs provide evidence to program review officers to close recommendations. PSPR Working Group officials stated that program review officers determine whether the RSO has provided adequate information to close a recommendation and may request documentation, if appropriate or applicable. However, OIG interviewed six officials who conduct PSPRs about the type of evidence they require to close a recommendation. Four officials stated that, depending on the recommendation, they would require evidence, such as photographs or documentation, to close a recommendation. One official stated that, depending on the recommendation, he would not require evidence as he trusts RSOs to address issues, and one official stated that a memorandum stating the post had addressed the recommendation was sufficient because the official did not expect RSOs to lie.

~~(SBU)~~ Because HTP officials are not receiving sufficient compliance documentation from RSOs about how recommendations were addressed, OIG found instances where HTP officials closed PSPR recommendations that were not fully addressed and were repeated in subsequent PSPR reports. Specifically, of 146 recommendations made to HTHR posts in FY 2018 and FY 2019, 8 (5 percent) were repeat recommendations. For example, the FY 2018 PSPR report for Embassy Niamey recommended that the local guard force orders be translated and posted at all guard posts. The RSO responded that "post created additional guard orders specific to each post. The orders were translated into French and placed at each posting." HTP officials closed this recommendation before the next PSPR. However, the FY 2019 PSPR team found that general guard orders at several guard posts were only in English and that no specific post guard orders appeared in English and French as previously recommended. The FY 2019 PSPR recommended, "RSO must ensure all [local guard force] binders contain current General and post specific Guard Orders in both English and French."

~~(SBU)~~ In another example, the FY 2018 PSPR report for Embassy Beirut recommended, "RSO should introduce language into the policy specifically stating RSO personnel have [Chief of Mission] authorization for use of government vehicles to provide 24-hour response capability." The RSO responded that the policy was updated to allow "RSO Special Agents to utilize government vehicles if/when dictated by exigent need." However, the PSPR team repeated the recommendation in the subsequent PSPR report: "RSO should work with the [Deputy Chief of Mission] to explicitly grant RSO personnel [Chief of Mission] authorization for use of Government vehicles for 24-hour response capabilities."

(U) DS officials stated that these recommendations were administratively closed and reissued. As a result of not receiving sufficient compliance documentation from RSOs, DS had limited assurance that HTHR posts resolved security deficiencies in a timely manner. Because of the security threats inherent to HTHR posts, more needs to be done to increase DS's assurance that the security deficiencies identified by PSPRs are fully resolved in a timely manner. OIG is, therefore, offering the following recommendation.

Recommendation 3: (U) OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to require regional security officers provide detailed, documented evidence that demonstrates corrective actions have been taken to remediate identified Post Security Program Review deficiencies and that those recommendations warrant closure.

(U) Management Response: DS concurred with the recommendation.

(U) OIG Reply: On the basis of DS's concurrence with the recommendation, OIG considers this recommendation resolved, pending further action. The recommendation will be closed when OIG receives and accepts documentation demonstrating that DS updated its PSPR policies and SOPs to require RSOs provide detailed, documented evidence that demonstrates corrective actions have been taken to remediate identified PSPR deficiencies and that those recommendations warrant closure.

(U) RECOMMENDATIONS

Recommendation 1: (U) OIG recommends that the Bureau of Diplomatic Security revise Post Security Program Review policies and standard operating procedures to include how the new application within the "RSO Tools" portal has been employed to track regional security officer compliance responses.

Recommendation 2: (U) OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to clarify requirements for following up on overdue responses from posts related to security deficiencies identified. The update should, at a minimum, include a process for notifying higher level post officials when responses are overdue, a process for tracking when responses are due, and a set schedule (with established intervals and milestones) for following up with posts.

Recommendation 3: (U) OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to require regional security officers provide detailed, documented evidence that demonstrates corrective actions have been taken to remediate identified Post Security Program Review deficiencies and that those recommendations warrant closure.

(U) APPENDIX A: BUREAU OF DIPLOMATIC SECURITY RESPONSE

United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

November 20, 2020

INFORMATION MEMO FOR ACTING INSPECTOR GENERAL KLIMOW – OIG

FROM: DS – Carlos F. Matus, Acting Senior Bureau Official

SUBJECT: Bureau of Diplomatic Security Response to the Office of Inspector General (OIG) Draft Management Assistance Report: The Bureau of Diplomatic Security's Compliance Process Related to Post Security Program Reviews Needs Improvement, Resulting from Audit of the Bureau of Diplomatic Security Post Security Program Review (PSPR) Compliance, AUD-SI-21-XXX

Below is the Bureau of Diplomatic Security (DS) response to OIG's draft report, including recommendations [#1-#3].

DS Response to Audit Finding and Recommendations:

DS proposes the following correction to the draft report:

DS launched a post security program review (PSPR) module housed within "RSO Tools" portal, a cloud-based application that will automate PSPR processes. The term "myRD" is used internally and not familiar to those outside of the International Programs (DS/IP) and High Threat Programs (DS/HTP) directorates. For this reason, we suggest solely referring to "RSO Tools" throughout the report instead of "myRD" (page 8, 10, and 13).

Recommendation #1: *OIG recommends that the Bureau of Diplomatic Security revise Post Security Program Review policies and standard operating procedures to include how myRD[sic] has been employed to track Regional Security Officer compliance responses.*

DS Response #1 (XX/XX/2020): DS concurs with this recommendation and will revise PSPR policies and standard operating procedures to include how RSO Tools has been employed to track Regional Security Officer compliance responses.

Recommendation #2: *OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to clarify requirements for following up on overdue responses from posts related to security deficiencies identified. The update should, at a minimum, include a process for notifying higher level post officials when responses are overdue, a process for tracking when responses are due, and a set schedule (with established intervals and milestones) for following up with posts.*

DS Response #2 (XX/XX/2020): DS concurs with this recommendation.

Recommendation #3: *OIG recommends that the Bureau of Diplomatic Security update its Post Security Program Review policies and standard operating procedures to require Regional*

Security Officers provide detailed, documented evidence that demonstrates corrective actions have been taken to remediate identified Post Security Program Review deficiencies and that those recommendations warrant closure.

DS Response #3 (XX/XX/2020): DS concurs with this recommendation.

Approved:	DS – Carlos F. Matus ()
Analyst:	DS/MGT/PPD – T. Carnell, ext. 5-3993
Drafted:	DS/HTP/RD – A. Madero DS/IP/RD – N. O'Donnell
Cleared:	DS/DSS – C. Matus, Acting (ok) DS/EX – W. Terrini (ok) DS/EX/MGT – J. Schools (ok) DS/MGT/PPD – T. Houser, Acting (ok) DS/MGT/PPD – L. Long (ok) DS/HTP – G. Sherman (ok) DS/HTP/RD – D. Cronin (ok) DS/IP – C. Chasten (ok) DS/IP/RD – M. Lombardo (ok)

(U) OIG AUDIT TEAM MEMBERS

Regina Meade, Director
Security and Intelligence Division
Office of Audits

Soraya Vega, Audit Manager
Security and Intelligence Division
Office of Audits

Christopher Yu, Auditor
Security and Intelligence Division
Office of Audits

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926
Stateoig.gov/HOTLINE

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