

DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats





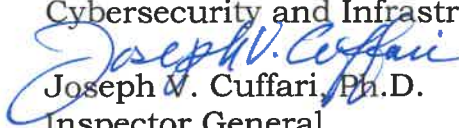
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

June 11, 2020

MEMORANDUM FOR: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

FROM: 
Joseph W. Cuffari, Ph.D.
Inspector General

SUBJECT: *DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats*

For your action is our final report, *DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving efforts to safeguard the commercial facilities sector. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider all of these recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.



DHS OIG HIGHLIGHTS

DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats

June 11, 2020

Why We Did This Audit

The shootings at an Orlando nightclub in June 2016 and a Las Vegas concert in October 2017 highlight the need to defend against attacks within the commercial facilities sector. Our audit objective was to determine the extent of DHS' efforts to deter and prevent terrorism or physical threats within the commercial facilities sector.

What We Recommend

We made three recommendations to improve the Department's coordination and outreach to safeguard the commercial facilities sector.

For Further Information:

For Further Information:
Contact our Office of Public Affairs at
(202) 981-6000, or email us at
DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Within the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA) is primarily responsible for working with components and partners to defend against current threats to the commercial facilities sector and build a more secure and resilient infrastructure. However, CISA does not effectively coordinate and share best practices to enhance security across the commercial facilities sector. Specifically, CISA does not coordinate within DHS on security assessments to prevent potential overlap, does not always ensure completion of required After Action Reports to share best practices with the commercial facilities sector, and does not adequately inform all commercial facility owners and operators of available DHS resources.

This occurred because CISA does not have comprehensive policies and procedures to support its role as the commercial facilities' Sector-Specific Agency (SSA). Without such policies and procedures, CISA cannot effectively fulfill its SSA responsibilities and limits its ability to measure the Department's progress toward accomplishing its sector-specific objectives. CISA may also be missing opportunities to help commercial facility owners and operators identify threats and mitigate risks, leaving the commercial facilities sector vulnerable to terrorist attacks and physical threats that may cause serious damage and loss of life.

CISA Response

CISA concurred with our recommendations. We have included a copy of CISA's response to our draft report in appendix A. We consider all three recommendations resolved and open.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security








Background

Our Nation's well-being relies on secure and resilient critical infrastructure. The Department of Homeland Security defines critical infrastructure as the physical and cyber assets and systems so vital to the United States that their incapacity or destruction would have a debilitating impact on the Nation's physical security, economic security, public health, or safety. Part of DHS' mission is to safeguard the Nation's many critical infrastructure sectors¹ from loss of life, property, and economic consequences.

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) identifies the commercial facilities sector as one of the Nation's critical infrastructure sectors. This sector includes privately-owned and operated facilities, such as retail spaces, office buildings, and sports stadiums. These facilities generally have open access, allowing the public to move freely without the deterrent of highly visible security barriers. Many commercial facilities are "soft targets and crowded places" that may be vulnerable to terrorist attacks or physical threats. The shootings at an Orlando nightclub in June 2016 (loss of 50 lives) and a Las Vegas concert in October 2017 (loss of 59 lives) are examples of attacks within the commercial facilities sector.

As shown in figure 1, the commercial facilities sector includes eight subsectors with facilities that have similar functions, operations, and security issues.

Figure 1: Commercial Facilities Subsectors

Entertainment & Media 49,024 establishments TV and movie production facilities, print media companies, and TV and radio broadcast stations \$1.4 trillion in total media spending annually 	Gaming 1,392 casinos and associated resorts Visited by 34% of U.S. adults in 2012 \$38 billion in tax revenue 	Lodging 52,887 hotel-based properties \$163 billion in annual sales 	Outdoor Events Fairs, exhibitions, outdoor venues, parades, and 564 amusement and theme parks 290 million visitors to amusement and theme parks in 2010 
Public Assembly 124,773 establishments stadiums, arenas, movie theaters, and cultural properties such as museums, zoos, libraries, and performance venues 	Real Estate Includes 1 million office buildings ¹ , 5.6 million multi-family rental buildings, and over 48K self-storage facilities Office buildings alone contribute \$205.1 billion to U.S. GDP each year 	Retail 1.1 million buildings malls, shopping centers, and retail \$2.5 trillion to U.S. GDP annually 	Sports Leagues 134 million attendees at games last season (top-four major sports leagues) The U.S. sports industry has an estimated size of \$485 billion 

Source: DHS' *Commercial Facilities Sector-Specific Plan*, 2015

¹ U.S. Presidential Policy Directive 21 identifies 16 critical infrastructure sectors: commercial facilities; chemical; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In October 2013, the then-Acting Secretary of Homeland Security designated the National Protection and Programs Directorate as the Department's Sector-Specific Agency (SSA) for commercial facilities under PPD-21. On November 16, 2018, the President signed the *Cybersecurity and Infrastructure Security Act of 2018* (Public Law 115-278), re-designating the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA). An SSA is a Federal department or agency responsible for leading, facilitating, or supporting the security and resilience programs and associated activities of a designated critical infrastructure sector.

The Department relies on CISA to work with other DHS components and partners to defend against threats and collaborate to build a more secure and resilient infrastructure, including commercial facilities, for the future. Table 1 outlines each DHS component's role in protecting commercial facilities.²

Table 1: DHS Organizations Involved in Protecting Commercial Facilities

DHS Component or Office	Role and Responsibility
CISA	Delivers infrastructure security services and capabilities, such as training and vulnerability assessments, to public and private sector stakeholders
Countering Weapons of Mass Destruction Office	Monitors for nuclear and biohazards during special events held at commercial facilities
Federal Emergency Management Agency (FEMA)	Assesses buildings to identify potential or existing vulnerabilities and provides training to external stakeholders
Office of Intelligence and Analysis	Shares intelligence information within the Department and with state, local, tribal, territorial, and commercial facility stakeholders
Office of Operations Coordination	Coordinates special events awareness, assesses risk of terrorist attack, and manages the appointments of Secretary appointed Federal Coordinators who are senior-level DHS officials that provide points of contact to support Federal, state, local, and private sector stakeholders
Office of Partnership and Engagement	Oversees the "If You See Something, Say Something®" campaign and other outreach efforts to stakeholders, such as the <i>Private Sector Resources Catalog</i>
Science and Technology Directorate (S&T)	Manages <i>Support Anti-Terrorism by Fostering Effective Technologies Act of 2002</i> (SAFETY Act) designations and certifications, including site visits to buildings
Source: DHS Office of Inspector General (OIG)-created based on audit interviews, document reviews, and DHS.gov	

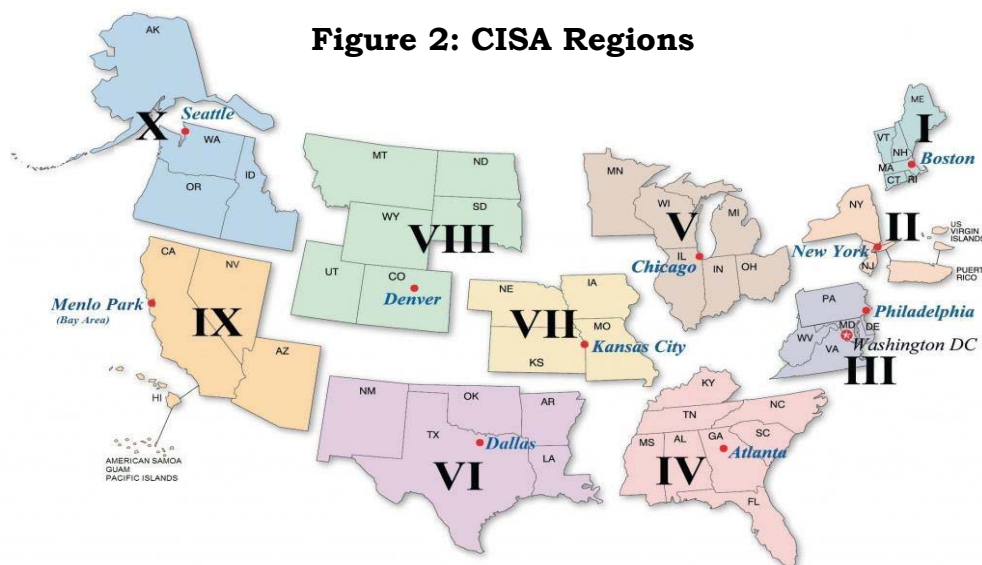
² Other DHS components — Transportation Security Administration, United States Coast Guard, and U.S. Customs and Border Protection — play a role in supporting special events, but were not included in the scope of this audit.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CISA's role as the SSA for commercial facilities includes providing outreach to commercial facility owners and operators. CISA's Protective Security Advisors (PSA) facilitate many of CISA's outreach and collaboration efforts to help protect commercial facilities. PSAs are trained security subject matter experts who facilitate activities in coordination with other DHS offices and components. They also advise and assist state, local, and private sector officials during routine, day-to-day operations and special events. PSAs have five mission areas: coordinate and conduct security surveys and assessments, conduct outreach activities, support special events, respond to incidents, and offer training. PSAs maintain field operations in 10 regions across the United States and its territories, as illustrated in figure 2. According to CISA, its PSA Program expended approximately \$44 million and had around 120 staff in fiscal year 2019.



Source: Office of Infrastructure Protection Regional Service Delivery Model, 2017

We conducted this audit to determine the extent of CISA's efforts to deter and prevent terrorism or physical threats within the commercial facilities sector.

Results of Audit

CISA Does Not Effectively Coordinate or Share Best Practices to Improve Security across the Commercial Facilities Sector

PPD-21 requires CISA, as the SSA, to coordinate DHS component activities to identify and disrupt threats to improve the security of the commercial facilities sector. To improve the security of this sector, DHS components such as CISA, S&T, and FEMA conduct various security assessments of buildings and venues



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

across the commercial facilities sector. The security assessments help owners and operators prevent, deter, and mitigate risks to their commercial facilities during daily operations and special events.

However, even though the assessments all covered similar security topics, CISA did not coordinate with the other DHS components, as required by PPD-21, to improve information sharing and prevent unnecessary duplication. For example, we reviewed site visit data for S&T and CISA between 2009 and 2018. We determined that S&T conducted site visits to 45 commercial facilities. CISA also visited 41 of the same sites, with 15 of the 41 (37 percent) visits performed between 2017 and 2018.³ We identified overlap in the facilities visited, as well as in some of the observations the components made during the site visits.

In addition, one of the goals in DHS' *Commercial Facilities Sector-Specific Plan*⁴ is to share security and resilience best practices to enable owners and operators to leverage lessons learned in all risk mitigation activities. CISA's PSAs learn of best practices through site visits, surveys, and other interactions with stakeholders. However, we found CISA's PSAs did not always share best practices related to outreach activities with each other. We interviewed 11 PSAs to determine how they shared lessons learned and best practices. Six of these 11 PSAs said there was no formal platform to share best practices with other PSAs. Although CISA personnel said they hold bi-monthly PSA calls to share best practices, our review of documentation supporting four bi-monthly calls in FY 2019 showed the calls included no such agenda items. Instead, these meetings focused on management changes to the program, operational updates, and administrative communications.

Further, although required, PSAs did not always share best practices for the commercial facilities sector after special events. PSAs are required to complete After Action Reports (AAR) after special events such as the Super Bowl or the Boston Marathon. When completed and disseminated, AARs are a critical tool the PSAs use to identify vulnerabilities and share best practices and lessons learned to improve security at future special events. For example, AARs we reviewed included best practices such as assigning PSAs to be on-site, having additional PSAs to appropriately cover large and geographically separated

³ FEMA conducts assessments of its own facilities, which could be either government-owned or commercial buildings, to identify potential or existing vulnerabilities. We could not compare FEMA's assessments for overlap or duplication because the component does not capture the necessary information in its system of record.

⁴ DHS' 2015 *Commercial Facilities Sector-Specific Plan* guides the sector's voluntary, collaborative efforts to improve security and resilience for 4 years. The plan describes how the commercial facilities sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in PPD-21. Additionally, this plan tailors the strategic guidance from the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

venues, and ensuring PSAs had access to systems for situational awareness and communication with other event stakeholders. We also determined that PSAs did not complete AARs for 14 of 19 (74 percent) special events sampled from FY 2016 through FY 2019. Specifically, CISA may have missed the opportunity to share lessons learned from high-profile events such as the 2016–2019 Boston Marathons, 2016 and 2017 Times Square New Year’s Eve events, and the 2018 National Mall Independence Day Celebration.

Finally, CISA did not inform all facility owners and operators of the variety of DHS resources available to help ensure sector security. According to the 2015 *Commercial Facilities Sector-Specific Plan*, PSAs are to inform and educate commercial facility owners and operators about threats from terrorism, the criticality of their facilities, and available DHS resources. However, 3 of the 21 stakeholders we interviewed said that although they knew about the local PSA, they were unaware of the DHS services available to them. In particular, 1 of the 3 stakeholders reported paying \$5,000 to contract for a site assessment, which a PSA could have performed free of charge.

CISA Does Not Have Adequate Policies and Procedures to Support Its Role as SSA for the Commercial Facilities Sector

CISA does not effectively coordinate or share best practices because it has not developed a comprehensive policy to effectively carry out its role as the SSA, that is, to lead, facilitate, and support security and resilience programs and associated activities across the Department. Although DHS published the 2015 *Commercial Facilities Sector-Specific Plan*, the plan was only designed to guide the sector’s voluntary, collaborative efforts and does not include specific procedures about how or when to coordinate and share best practices across the Department. Including specific requirements and performance measures is critical for CISA to measure the Department’s progress toward accomplishing its sector-specific activities.

CISA also did not develop procedures for updating sector resources with relevant threat information. According to the *Commercial Facilities Sector-Specific Plan*, CISA must ensure the sector has access to timely, actionable, and threat-specific information and analysis. However, the plan does not include a process or specific timeframes for updating these critical tools and resources. It only includes a requirement to update the *Commercial Facilities Sector-Specific Plan* every 4 years.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

For instance, during the audit we identified outdated tools and resource guides. We found that CISA's site surveys, which it conducts to identify commercial facilities' physical security, protective measures, and security gaps, have not been updated with new or relevant information since 2014. The surveys did not include updated security procedures or threats identified during recent attacks such as the concert shooting in Las Vegas, the vehicle ramming in New York City, or the Orlando night club shooting. (See figure 3.)

Additionally, the *Private Sector Resources Catalog*, published by DHS' Private Sector Office within the Office of Partnership and Engagement, had not been updated in about 7 years. The catalog centralizes access to DHS' private sector resources that help prevent terrorism, enhance security, and ensure resilience to hazards and threats. In January 2020, the Private Sector Office released a new *Private Sector Resources Catalog*, with updates to occur every 2 years.

In addition, CISA does not have a procedure requiring its management to use data on PSA outreach efforts to inform decision making. PPD-21 directs CISA to use analytic functions to inform planning and operational decisions. Further, according to the Government Accountability Office, using data to drive decision making can help Federal agencies improve program implementation, identify and correct problems, and help make other critical management decisions. However, CISA does not use data collected during outreach efforts to inform decisions regarding the PSA program. Instead, CISA uses informal ad hoc decision making to determine where to allocate PSA resources and ensure the subsector coverage needed.

Although we acknowledge DHS' efforts to develop the *Commercial Facilities Sector-Specific Plan*, it does not contain specific policies and procedures. Without such policies and procedures, CISA cannot effectively carry out its SSA responsibilities and is limited in its ability to measure the Department's progress toward accomplishing sector-specific activities. Further, CISA may be missing opportunities to help commercial facility owners and operators identify threats and mitigate risks, leaving the commercial facilities sector vulnerable to terrorist attacks and physical threats that may cause serious damage and loss of life.

Figure 3: Recent Attacks



Source: Images from public websites



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendations

Recommendation 1: We recommend the Director, Cybersecurity and Infrastructure Security Agency, work with the Acting Secretary, Department of Homeland Security, to develop comprehensive policies and procedures to support its role as the commercial facilities' Sector-Specific Agency. Specifically:

- a. provide convening authority and clear expectations to ensure the agency can fulfill its responsibility as the designated Sector-Specific Agency;
- b. develop methods to share best practices;
- c. ensure effective coordination across the Department's components and update all critical resource documents—including the *Private Sector Resource Catalog*—as required; and
- d. develop procedures to ensure comprehensive analysis of data.

Recommendation 2: We recommend the Director, Cybersecurity and Infrastructure Security Agency, develop and implement a process to oversee completion of required report reviews, including After Action Reports for supporting special events.

Recommendation 3: We recommend the Director, Cybersecurity and Infrastructure Security Agency, develop policy and a process to review and update the site security survey methodology and tool annually.

Management Comments and OIG Analysis

CISA concurred with the recommendations. We consider all recommendations resolved and open. Appendix A contains a copy of CISA's comments in their entirety. CISA submitted technical comments separately, which we incorporated in the report as appropriate. The following is a summary of DHS' response to each recommendation and OIG's analysis of those responses.

CISA's Response to Recommendation 1: Concur. CISA agreed that integrating the development of new and updated policies and procedures will enhance its SSA capabilities. CISA will pursue the development of recommended policies, procedures, and best practices for optimal execution of SSA responsibilities as an appendix to the next version of the National Infrastructure Protection Plan. The estimated completion date is December 31, 2020.

OIG Analysis: This recommendation is resolved and open. We consider the planned actions responsive to the recommendation. We will close the recommendation when CISA provides documentation showing the agency



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

developed comprehensive policies and procedures to support its role as the commercial facilities' SSA.

CISA's Response to Recommendation 2: Concur. CISA will establish an after-action program to consistently assess its special event security support. Each AAR will include an overview of CISA's support for an event as well as recommendations for enhancing capabilities to better support special event organizers. The estimated completion date is January 29, 2021.

OIG Analysis: This recommendation is resolved and open. We consider CISA's planned actions responsive to the recommendation. We will close the recommendation when CISA provides documentation showing the agency established the after-action program and examples of the new AARs.

CISA's Response to Recommendation 3: Concur. CISA will create a routine procedure to provide the guiding principles for the new process, identify goals and responsibilities of the principal parties, and delineate required documentation and timeframes. CISA did not agree with updating the site survey annually. However, the agency agreed to routine updates every other year. The estimated completion date is December 31, 2020.

OIG Analysis: This recommendation is resolved and open. CISA uses its site surveys to identify commercial facilities' physical security, protective measures, and security gaps. The site survey tool has not been updated with new or relevant information since 2014. Therefore, the site survey tool did not include updated security procedures or threats identified during recent attacks. We will close the recommendation when CISA provides evidence that the agency is routinely reviewing and updating its site survey tool to meet the intent of the recommendation to keep the tool current.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent of CISA's efforts to deter and prevent terrorism or physical threats within the commercial facilities sector. To answer our objective we obtained, reviewed, and analyzed Federal, departmental, and component documents and information including, but not limited to:

- legislation, policies, procedures, and guidance related to the protection of commercial facilities



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- CISA operating and strategic plans
- CISA performance plans
- *Commercial Facilities Sector-Specific Plan*
- *Soft Targets Crowded Places Plans and Resource Guide*
- *Private Sector Resources Catalogs*
- site visit and assessment data
- AARs
- budget and funding information
- prior OIG and Government Accountability Office reports
- media articles
- congressional testimony

Our audit scope included FYs 2016 through FY 2019. We also analyzed all CISA and S&T site visit data as reported through FY 2018. We reviewed special events and supporting documentation for events occurring from January 2016 through April 2019. We conducted more than 70 interviews with DHS personnel from the components and offices in table 1, at both headquarters and field locations.

We conducted site visits to meet with DHS officials, state and local organizations, and commercial facility owners and operators in the following locations: Florida, Georgia, Illinois, Massachusetts, Nevada, New Jersey, Pennsylvania, Texas, Virginia, and Washington, D.C. We judgmentally and randomly selected CISA PSAs to interview based on location and availability. We also interviewed approximately 35 judgmentally selected commercial facility owners and operators based on location and from all eight commercial facility subsectors nationwide, such as sports venues, convention centers, and casinos.

As part of our review, we evaluated DHS' actions to protect the commercial facilities sector. We also assessed the effectiveness of the assistance DHS provided to commercial facility stakeholders to identify risks and shortcomings through interviews judgmentally selected based on location and availability. We observed CISA carrying out its role during day-to-day operations and special events. We also attended five special events, including the 2018 Chicago Marathon, Super Bowl LXIII, a Major League Soccer game in Orlando, an amusement park's half marathon, and the 2019 Boston Marathon, between October 2018 and April 2019, which we judgmentally selected based on the time, location, size, and nature of the event. We observed training, such as Active Shooter and Improvised Explosive Device awareness, as well as tabletop exercises supported by DHS components. These training events were selected based on local availability during site visits.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We obtained and analyzed computer-processed data on the number of site visits performed on commercial facilities. We used this data for our sample selection of external commercial facilities interviews and site visit testing. To assess the reliability of this data, we interviewed agency officials knowledgeable about the information and traced and verified the data for completeness and accuracy. Although we identified issues with the data's completeness and accuracy, they did not materially impact our findings.

We obtained and evaluated funding data for CISA's PSA Program. We attempted to track CISA's budget allocations to the commercial facilities sector level. However, CISA does not track funds to the sector level. We reported this information as provided for background context, but did not use it to support our overall conclusions and recommendations. We also used FY 2016 through FY 2019 special event data, which we obtained directly from the Homeland Security Information Network, to create a judgmental sample of special events to observe and AARs to review. We reviewed the special event data for reasonableness but did not test the overall reliability of this system as it was only used for sampling purposes. We verified the reliability of the data systems, such as Infrastructure Protection Gateway and the SAFETY Act of 2002 Management System, used during the audit through interviews, emails, and screenshots. Overall, the data included in this report was sufficiently reliable to support our conclusions.

We conducted this performance audit between June 2018 and January 2020 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We consider the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objective.

The Office of Audits major contributors to this report are Patrick O'Malley, Director; Stephanie Brand, Audit Manager; Christine Meehan, Auditor-In-Charge; Junior Correa, Auditor; Andrew Herman, Auditor; Ebenezer Jackson, Program Analyst; Kristine Odiña, Program Analyst; Lindsey Koch, Communications Analyst; Stefanie Holloway, Independent Referencer.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
CISA Comments to the Draft Report

U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Washington, DC 20528



CISA
CYBER-INFRASTRUCTURE

May 28, 2020

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "DHS Can Enhance Efforts to Protect Commercial Facilities from Terrorism and Physical Threats" (Project No. 18-075-AUD-FEMA, NPPD)

Thank you for the opportunity comment on this draft report. The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA is committed to the security of commercial facilities and has worked closely with industry for over a decade to develop programs to reduce risk and share best practices across the sector. In 2017, DHS established the Soft Targets-Crowded Places (ST-CP) Executive Steering Committee (ESC), which CISA chairs, to coordinate Department-wide activities in support of commercial facilities. CISA has also established a Security Programs office to focus on developing products and services for CISA regional staff to deliver to commercial facilities partners across the country. CISA will continue to improve coordination and outreach to safeguard commercial facilities and remains committed to the safety and protection of commercial facilities from terrorism and physical threats.

The draft report contained three recommendations with which CISA concurs. Attached find our detailed response to each recommendation. CISA previously submitted technical comments under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Attachment: Management Response to Recommendations Contained in OIG-18-075-AUD-FEMA, NPPD

OIG recommended that the CISA Director:

Recommendation 1: Work with the Acting Secretary, Department of Homeland Security, to develop comprehensive policies and procedures to support its role as the commercial facilities' Sector-Specific Agency. Specifically:

- a. provide convening authority and clear expectations to ensure the agency can fulfill its responsibility as the designated Sector-Specific Agency [SSA];
- b. develop methods to share best practices;
- c. ensure effective coordination across the Department's components and update all critical resource documents—including the Private Sector Resource Catalog—as required; and
- d. develop procedures to ensure comprehensive analysis of data.

Response: Concur. CISA agrees that integrating the development of new and/or updated policies and procedures will enhance the capabilities across all critical infrastructure sectors for which it serves the SSA. However, this development of any new and/or updated comprehensive policy and supporting doctrine should be closely aligned with the overall framework of the National Infrastructure Protection Plan (NIPP). The NIPP provides the guiding principles supporting effective collaboration between private and public sector partners and serves as a fundamental reference for all SSAs to fulfill their roles. Moving forward, CISA's Stakeholder Engagement Division will pursue the development of recommended policies, procedures, and best practices for optimal execution of SSA responsibilities as an appendix to the next version of the NIPP. Estimated Completion Date (ECD): December 31, 2020.

Recommendation 2: Develop and implement a process to oversee completion of required report reviews, including After Action Reports for supporting special events.

Response: Concur. Through Protective Security Advisors (PSAs) and other regional resources, CISA provides comprehensive support to commercial facility partners in preparation for special events. Specifically, CISA provides security site surveys, more than 350 immersive video captures, and training. CISA continuously builds upon its resources and processes to enhance stakeholder security capacity building across the country with emphasis on a wide range of Special Event Assessment Rating engagements. To further augment the PSA Special Event Working Group, which CISA established over three years ago to broadcast effective practices; CISA's Integrated Operations Division will establish an after-action program to consistently assess its direct support to special event security. These after-action reports will include an overview of



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

the support provided by CISA, as well as recommendations for enhancing organizational capabilities to better support special event organizers with their risk mitigation efforts. ECD: January 29, 2021.

Recommendation 3: Develop policy and a process to review and update the site security survey methodology and tool annually.

Response: Concur. The development of a new policy and associated procedure for reviewing and updating—as necessary—the site security survey methodology and tool will enhance the Department’s credibility with critical infrastructure owners and operator, as well as Federal, State, local, tribal, and territorial government partners. Consequently, CISA’s Infrastructure Security Division (ISD) will develop this procedure through coordination across the CISA enterprise to ensure consistency with other similar requirements. Once complete, this procedure will: (1) provide the guiding principles for the review process; (2) identify the roles and responsibilities of the principal parties; and, (3) delineate the required documentation and timeframes.

It is important to note, however, that updating the site security survey methodology and tool is not necessarily needed annually; especially if a future methodology and tool shows that it improved the Department’s credibility with critical infrastructure owners and operators other partners. Instead, CISA believes that a review, with potential updates, should occur every other year. ISD will work with the OIG to come to an agreement as to what makes the most sense regarding the appropriate frequency of reviewing and updating the site security survey methodology and tool. ECD: December 31, 2020.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B

Report Distribution

Department of Homeland Security

Acting Secretary
Senior Official Performing the Duties of the Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, Government Accountability Office/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director, Cybersecurity and Infrastructure Security Agency
CISA Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305