U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-62 September 27, 2024

FINAL REPORT

DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | *www.oig.dhs.gov*

September 27, 2024

MEMORANDUM FOR: Eric N. Hysen
Chief Information Officer
Department of Homeland Security

Christopher J. Tomney
Director
Office of Homeland Security Situational Awareness

Kenneth L. Wainstein
Under Secretary
Office of Intelligence and Analysis

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

GLENN E SKLAR Digitally signed by GLENN E SKLAR Date: 2024.09.27 12:10:55 -04'00' *for*

SUBJECT: *DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information*

Attached for your action is our final report, *DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving partners' use of DHS technology to obtain emerging threat information. Your office concurred with two of the four recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 and 2 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.

Recommendations 3 and 4 are open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status

of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Please send your response 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 DHS. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General, Office of Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information

September 27, 2024

Why We Did This Audit

The *Homeland Security Act* requires DHS to provide situational awareness and a common operating picture for the entire Federal Government — and for state, local, and tribal governments as appropriate — in the event of a natural disaster, act of terrorism, or other man-made disaster. Recent incidents and disasters highlighted the need for situational awareness throughout the Homeland Security Enterprise. We conducted this audit to determine whether DHS has technology to identify and share actionable information on emerging threats with its external partners.

What We Recommend

We made four recommendations to increase DHS partners' awareness of emerging threats and use of information sharing technologies.

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

The Department of Homeland Security has technology that enables identification and sharing of emerging threat information, but DHS partners did not always use this technology to obtain threat information. DHS has various technological methods for maintaining real-time situational awareness and identifying threat information, such as the Office of Homeland Security Situational Awareness' media monitoring and a virtual situation room. DHS shares this information via its Homeland Security Information Network (HSIN). However, DHS partners often did not leverage HSIN for information sharing. According to the Office of the Chief Information Officer's data, more than half of the 55,609 active HSIN account holders did not log into HSIN between March 22 and September 15, 2023. Instead, partners such as fusion centers and other external partners relied on their own systems and commercially available products to obtain and share information in real time. Additionally, partners were not always aware of HSIN modernization or training efforts.

Partners did not always fully leverage DHS technologies because a lack of HSIN functionality hindered its use; DHS did not conduct outreach to support partners' HSIN mission needs; and DHS did not always share information with partners in a timely manner.

As a result, DHS cannot always effectively share emerging threat information with partners, which may limit DHS and its mission partners' response to emerging threats against the homeland.

Department Response

The Department concurred with two recommendations and did not concur with two recommendations.

Table of Contents

Abbreviations

CIO	Chief Information Officer
COP	common operating picture
HSE	Homeland Security Enterprise
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
NOC	National Operations Center
OSA	Office of Homeland Security Situational Awareness
U.S.C.	United States Code
vSITROOM	Virtual Situation Room

Background

The Department of Homeland Security's mission includes ensuring the homeland is safe, secure, and resilient against all threats to public safety and critical infrastructure. The *Homeland Security Act of 2002* assigned DHS responsibility for coordinating the Federal Government's homeland security communications with state and local governments and the private sector. The Act also assigned DHS responsibility for establishing an information technology infrastructure (i.e., system), for sharing homeland security information with its Federal, state, local, and private sector partners. Recent incidents and disasters, such as civil unrest, a mass shooting in Maine in October 2023, and severe storms and flooding throughout the Nation, highlight the need for situational awareness throughout the Homeland Security Enterprise (HSE),[1] including among fusion centers and private sector partners. To successfully combat threats against the homeland, DHS must share emerging threat information with its partners.[2]

Within DHS, the Office of Homeland Security Situational Awareness (OSA) oversees the National Operations Center (NOC), which is responsible[3] for ensuring critical terrorism and disaster-related information reaches government decision-makers. OSA's mission is to provide situational awareness, a common operating picture[4] (COP), and decision support for the HSE on threats,[5] incidents, hazards, and events impacting the homeland. The *Homeland Security Act of 2002*, as amended, designated OSA's NOC as the principal operations center for the Department and requires the NOC to provide situational awareness and a COP for Federal, state, local, tribal, and territorial government partners for incidents, events, and threats involving natural disasters, acts of terrorism, or other man-made disasters.

DHS' Office of Intelligence and Analysis (I&A) specializes in sharing intelligence and analysis with decision-makers to identify and mitigate threats to the homeland. I&A is statutorily charged[6] with providing intelligence to its partners. I&A's mission is to equip the HSE with timely intelligence and information to keep the homeland safe, secure, and resilient. I&A personnel are

[1] According to DHS, the HSE is the collective efforts and shared responsibilities to maintain critical homeland security capabilities and includes Federal, state, local, tribal, and territorial governments; non-governmental, private-sector, and international partners; and individuals, families, and communities.
[2] DHS defines a partner as an outside entity that participates in a project as a source of operational requirements, testing support, solution providers, co-researchers/developers, or other support functions. This report uses the word partner when referring to Federal, state, local, territorial, tribal, and other partners external to DHS.
[3] See 6 United States Code (U.S.C.) § 321d, *National Operations Center*.
[4] DHS' Science and Technology Directorate defines COP as "a continuously updated overview of an incident compiled throughout an incident's life cycle from data shared between integrated communication, information management, and intelligence and information sharing systems. The goal of a COP is real-time situational awareness across all levels of incident management and across jurisdictions."
[5] We considered emerging threats to be forthcoming or active attacks against the homeland. DHS defines a threat as an "indication of potential harm to life, information, operations, the environment and/or property."
[6] See 6 U.S.C. § 124h(b)(1), *Department of Homeland Security State, Local, and Regional Fusion Center Initiative*.

assigned to all 80 fusion centers,[7] which are state-owned and operated focal points for the receipt, analysis, gathering, and sharing of threat-related information between Federal, state, local, tribal, territorial, and private sector partners. The NOC can also share threat information with I&A staff and fusion centers.[8]

According to the NOC, its primary source of threat information is from the Intelligence Community through I&A, and its primary indication that an incident may have occurred is from traditional and social media monitoring, via its media monitoring analysts. The NOC's contracted analysts for media monitoring share information with the NOC and HSE partners. Appendix C provides an overview of the NOC's information sharing process. The NOC also provides and maintains tools to facilitate information sharing with partners, such as a DHS COP,[9] and a virtual situation room (vSITROOM),[10] which is located within the Homeland Security Information Network (HSIN).

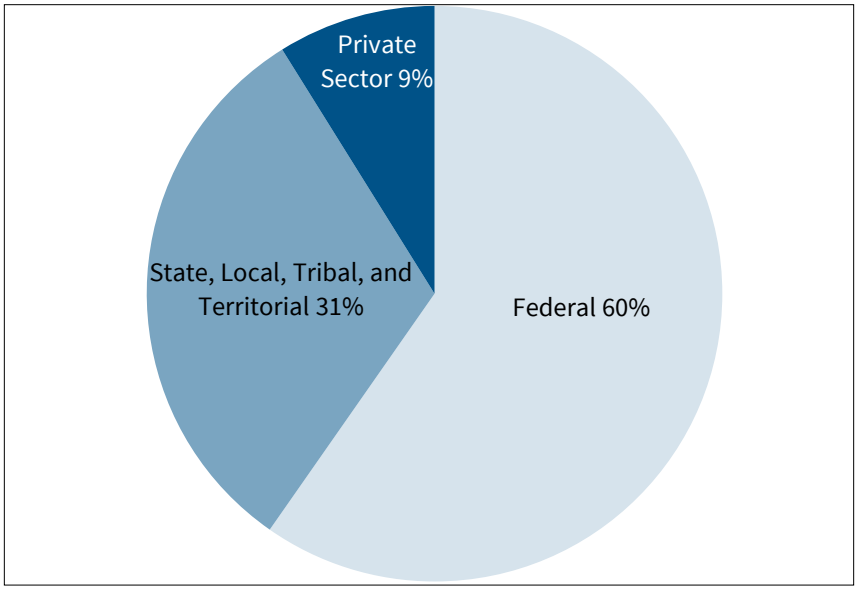
HSIN is DHS' primary system, managed by the DHS Office of the Chief Information Officer (CIO), for sharing information with partners. OSA, the NOC, I&A, fusion centers, and other external partners can use DHS' HSIN and other technologies to share information. Partners use HSIN to access homeland security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information needed to fulfill mission requirements. According to Office of the CIO data, between March 22 and September 15, 2023, HSIN's 55,609 active account holders comprised:

- 27,139 Federal account holders;
- 14,281 state, local, tribal, and territorial account holders;
- 4,036 private sector account holders;
- 451 international account holders; and
- 9,702 account holders whose accounts are not associated with sectors.

Figure 1 details active HSIN account holders by group.

[7] Fusion centers are located in all 50 states and some U.S. territories.
[8] The NOC and I&A are collocated to share information.
[9] The NOC's COP is part of an unclassified platform that displays incident dashboards, including weather-related incidents.
[10] The vSITROOM is the NOC's 24/7 HSIN-based platform for real-time information sharing.

Figure 1. Percentages of Each Active HSIN Account Holder[11]



Source: The Office of the CIO provided HSIN account holder data as of September 2023

Despite the number of active account holders, DHS and partner use of HSIN to share information has historically been limited. In 2013, we reported that HSIN had "not been used to share information widely across the HSE," despite having 35,560 active account holders in October 2012.[12] The audit team determined HSIN use was limited in part because system content was not useful to partners and the system was not user-friendly. Similarly, we reported in 2006[13] that state and local partners did not regularly use HSIN and instead used other methods to share information.

We conducted this audit to determine whether DHS has technology to identify and share actionable information on emerging threats with its external partners.

[11] Figure 1 is not representative of all 55,609 active HSIN account holders between March 22 and September 15, 2023. Figure 1 does not include the 451 active international account holders or 9,702 active account holders whose accounts are not associated with sectors.
[12] *Homeland Security Information Network Improvements and Challenges,* OIG 13-98, June 2013.
[13] *Homeland Security Information Network Could Support Information Sharing More Effectively,* OIG 06-38, June 2006.

Results of Audit

DHS has technology that enables identification and sharing of emerging threat information, but DHS partners did not always use this technology to obtain threat information. DHS has various technological methods[14] for maintaining real-time situational awareness and identifying threat information, such as OSA's media monitoring and the vSITROOM. DHS shares this information via its HSIN. However, DHS partners often did not leverage HSIN for information sharing. According to the Office of the CIO's data, more than half of the 55,609 active HSIN account holders did not log into HSIN between March 22 and September 15, 2023. Instead, partners such as fusion centers and other external partners relied on their own systems and commercially available products to obtain and share information in real time. Additionally, partners were not always aware of HSIN modernization or training efforts.

Partners did not always fully leverage DHS technologies because a lack of HSIN functionality hindered its use; DHS did not conduct outreach to support partners' HSIN mission needs; and DHS did not always share information with partners in a timely manner.

This limits use of and reliance on DHS information sharing technologies. As a result, DHS cannot always effectively share emerging threat information with partners, which may limit DHS and its mission partners' response to emerging threats against the homeland.

DHS Uses Various Technologies to Identify Threats and Maintain Situational Awareness

DHS has a number of technologies to help identify[15] emerging threats, such as its contract for media monitoring and the vSITROOM. These technologies enable DHS analysts to identify and maintain situational awareness of threats via data mining and open-source monitoring, such as monitoring social media. The NOC's media monitoring analysts provide the NOC with advance notice of media reporting, primarily via the vSITROOM chatroom and secondarily via telephone. The contracted analysts also notify partners via email of relevant media alerts. DHS components and external partners can also leverage these technologies to identify threat information. The NOC conducts daily unclassified coordination calls to facilitate information sharing among partners, including unclassified threat information. The vSITROOM also facilitates threat identification via the chatroom.

Based on our audit work, interviews, and observations of the NOC and the vSITROOM, we determined these technologies generally increased effective situational awareness throughout

[14] I&A uses multiple technologies, including HSIN, to share information.
[15] The NOC is located in Washington, DC, and does not identify incidents or emerging threats in the field. The NOC is DHS' primary mechanism to gather and share emerging threat information.

the HSE for potential threats. Examples of threat information identified include a mass casualty event at a concert in Texas,[16] a car driving through a parade in New Mexico,[17] and bomb threats to multiple colleges and universities across the Nation in July 2022.[18]

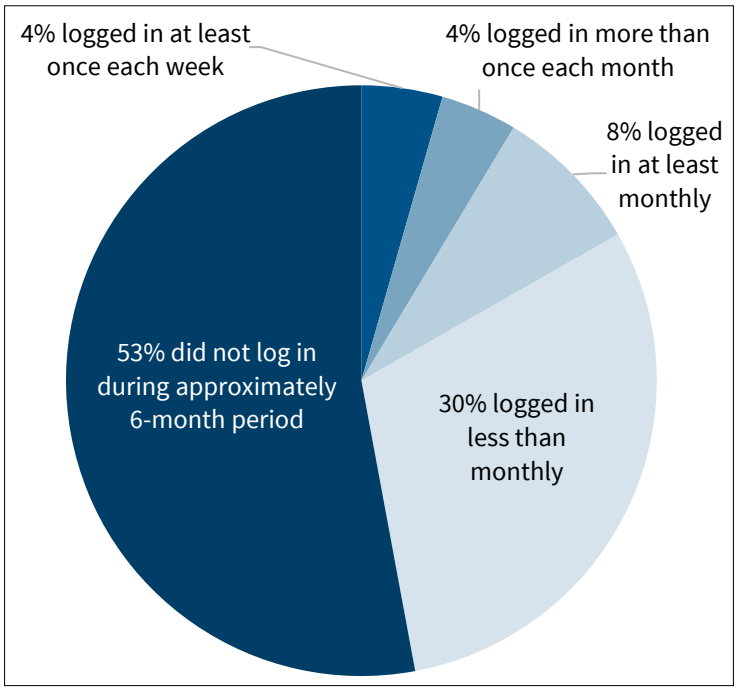
Partners Did Not Always Fully Leverage DHS Information Sharing Technologies

The *Homeland Security Act*[19] requires OSA's NOC to provide its partners with situational awareness and a COP to ensure critical terrorism and disaster-related information reach governmental and non-governmental decision-makers. According to the NOC's *Standard Operating Procedure,*[20] the NOC provides a U.S. Government-wide COP, national-level situational awareness, and coordination for the efforts of the Department with other agencies and state and local governments to prepare for, prevent, respond to, and recover from natural and man-made disasters. This procedure states the NOC is to facilitate shared situational awareness across the HSE. To share threat information, OSA and the NOC use HSIN, as well as the COP, the vSITROOM, phone, and email.

Despite HSIN being DHS' primary system for sharing information with partners, more than half of the HSIN account holders did not regularly use the platform. According to Office of the CIO data, between March 22 to September 15, 2023, there were 55,609 active HSIN account holders; of these, 29,427 (53 percent) did not log into HSIN within approximately 6 months,[21] as shown in Figure 2.

[16] The NOC's media monitoring analysts provided the NOC with incident information regarding a concert in Texas in November 2021 where 10 people died and many more were injured.
[17] The NOC's media monitoring analysts provided the NOC with incident information regarding a parade in New Mexico in August 2022 where a person drove a car through the parade route, injuring at least 15 people.
[18] The NOC's media monitoring analysts provided the NOC with threat information regarding bomb threats to multiple colleges and universities in several states on a single day in July 2022.
[19] See 6 U.S.C. § 321d, *Domestic Security*.
[20] The NOC's *Standard Operating Procedure*, December 2021.
[21] 26,182 active HSIN account holders logged into HSIN between March 22, 2023, and September 15, 2023. The Office of the CIO provided only partial HSIN account holder login data prior to March 22, 2023.

Figure 2. Frequency of Active HSIN Account Holder Logins for Partners[22]



Source: The Office of the CIO provided HSIN account holder login data between March 22, 2023, and September 15, 2023

In addition to the more than 29,000 active account holders who had not logged in for approximately 6 months, as of September 2023, the Office of the CIO reported it has deactivated 164,195[23] HSIN accounts within approximately the last 7 years. The Office of the CIO deactivates HSIN accounts when account holders request deactivation or when account holders' access lapses due to login inactivity for 365 days. According to data the Office of the CIO provided, 155,728, or 95 percent, of the 164,195 deactivated accounts were due to login inactivity for 365 days. We reported[24] similar limited HSIN logins of state and local officials in 2006.

The NOC's platforms may not be fully utilized. We observed the NOC's vSITROOM operations on multiple occasions and during incidents, such as active shooters, and special events, such as marathons, and noted only a marginal increase in users monitoring the room. During our

[22] The percentages in Figure 2 sum to 99 percent instead of 100 percent because we rounded each sector's active HSIN account holder logins to the nearest whole percent.
[23] The Office of the CIO was not able to provide deactivation dates for all deactivated HSIN accounts. According to the Office of the CIO, it deactivated most of the 164,195 deactivated HSIN accounts as of 2022.
[24] *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG 06-38, June 2006.

observations, we noted only approximately 50 users[25] in the NOC's vSITROOM nationwide, even during incidents when we anticipated increased information sharing activity. For example, we observed 51 HSIN users in the vSITROOM during an active shooter incident in Maine, 48 HSIN users in the vSITROOM during the Superbowl, and 63 HSIN users in the vSITROOM during a United Nations General Assembly.

Fusion centers often relied on their own sources of information, in addition to HSIN, to obtain threat information. All 11 fusion centers we met with did use HSIN to receive threat information. However, fusion centers have their own analysts, and some have their own social media monitoring contracts. Fusion centers also relied primarily on their own systems and commercially available products, including business messaging applications, email, and text messaging, to share information in real time. One fusion center piloted its own virtual, real-time information sharing platform for fusion centers and other partners to use during significant events instead of using HSIN and the NOC's COP or vSITROOM. Further, some fusion centers did not use the NOC's COP or vSITROOM at all.

Not all external partners we met with used HSIN. Specifically, of the 18,300 state, local, tribal, territorial, and private stakeholder active HSIN account holders, more than 8,000 had not logged into the system in more than 6 months as of September 15, 2023. Further, 6 of the 16 non–fusion center external partners interviewed did not use HSIN. Instead of using HSIN, one external partner reported using email and other means to communicate and share threat information. Another external partner could not gain access to HSIN features and did not know whom to contact to resolve the issue.

Finally, we surveyed all active HSIN account holders (1,027) external to DHS to rate HSIN on a scale from 0 to 10, with 10 being the best. The most selected number, with more than 20 percent of responses was 5 of 10. The average score was 6.2 of 10. See Appendix D for survey details.

Not All DHS Partners Were Aware of HSIN Modernization and Training Efforts

Despite the Office of the CIO's plans to modernize HSIN to improve system functionality in fiscal year 2025,[26] most account holders were not aware of these improvement plans. In 2022, DHS proposed and received more than $26 million in funding to rebuild HSIN's underlying platform, enhance HSIN's user interface, and expand mobile solutions for state and local partners. As a part of the modernization effort, the

80 percent of active HSIN account holder survey respondents were not aware of HSIN modernization efforts.

[25] Users include both individual users and organizations. Users could be partner operations centers or partner watch floors.

[26] According to the Office of the CIO, its plans to modernize HSIN will expand search functions, discoverability, and the mobility of documents, and improve the registration and login processes.

Office of the CIO plans to consider feedback from HSIN account holders to determine what enhancements it should implement to improve system usability. Most active HSIN account holders external to DHS we surveyed were unaware of the Office of the CIO's modernization efforts. As of April 2024, the Office of the CIO could not specify an estimated timeframe for modernization completion.

The Office of the CIO promotes and shares HSIN training opportunities, updates, and news during its monthly HSIN user group meetings, via its bimonthly bulletin, and through HSIN Learn. Of those account holders who participated in HSIN training, 87 percent of survey respondents found the training helpful. Despite this positive feedback, our survey of active HSIN account holders external to DHS showed 42 percent of respondents were not aware of available training. Additionally, several partners interviewed were unaware of topics discussed in recent HSIN bimonthly bulletins, including HSIN training opportunities and the HSIN user group.

Lack of HSIN System Functionality, Outreach, and Timely Information Sharing Hindered Partners' Use of DHS Technology

Several factors hindered DHS and its partners' use of HSIN to share threat information. Issues with system functionality limited partners' use of HSIN. Also, a lack of outreach to create awareness of HSIN resources, including HSIN features, modernization, and training opportunities, limited partners' use of HSIN. Partners reported shared information was not always useful because DHS did not always share threat information in a timely manner.

Lack of HSIN System Usability and Functionality Hindered Partner Use

Based on congressional requirements to improve HSIN usability and search functionality,[27] DHS expended more than $38 million on HSIN operations and maintenance since 2021. We found 447, or 44 percent, of 1,027 respondents we surveyed identified challenges with the system's ease of use. One survey participant responded, "Ease of use is probably the most negative thing with HSIN. The relevant information is there, it is just extremely difficult to find." According to personnel at one fusion center we visited, their law enforcement partners avoided using HSIN because it is not user-friendly. In 2013, we also reported challenges with HSIN's user-friendliness.[28] Specifically, we reported that users "could not easily locate information in HSIN." Users found browsing through the folders in the document library confusing and unhelpful for discovering new information that might be useful to them. In addition, our 2013 report noted users could not easily find information on HSIN using the search function. Search results often

[27] 6 U.S.C. § 121, *Information and Analysis,* directed DHS' CIO, in consultation with the Chief Intelligence Officer, to "assess and implement, as appropriate, technical enhancements to HSIN to improve usability, including search functionality, data analysis, and collaboration capabilities."
[28] *Homeland Security Information Network Improvements and Challenges,* OIG 13-98, June 2013.

did not contain the specific documents that users were looking for, which they had previously seen on HSIN.

Based on our survey of deactivated account holders, 124 respondents identified HSIN not being user-friendly as the sole reason they no longer use the platform. Partners identified the following challenges with HSIN:

- Despite Congress specifically requiring DHS to upgrade HSIN's search capabilities, an active HSIN account holder respondent said, "It feels old and clunky, the search functionality is limited, and the interface is not intuitive at all." The respondent further explained, "HSIN should feel as natural as platforms most people use day in and day out…the harder the platform is to figure out, the less people will use it." Six partners interviewed at various locations referred to HSIN as "clunky." Another survey respondent said, "I am not really able to find the information I want. Even though I have been on HSIN for 10 years and have uploaded many documents, a search for my own name comes up with nothing."

- HSIN's mobile platform did not perform well. Some partners reported losing connection to HSIN on their mobile device when receiving phone calls. Further, partners noted HSIN Connect did not perform well on mobile devices.

- HSIN users already logged into a HSIN website cannot open links to documents directly from an emailed link. Instead, they must click on the HSIN document's link from the email and login to HSIN again to view the document. A representative from one partner said, "you can log into your bank easier and quicker than HSIN."

HSIN users also experienced challenges logging into the platform. According to the Office of the CIO, HSIN user logins varied because users' needs for HSIN were not consistent. Some users only used HSIN during planned special events, while incidents were ongoing, or during a specific period, like hurricane season. Account holders reported difficulty accessing the system and general usability issues as reasons for limited HSIN use. Specific to system access, 371, or 36 percent, of the 1,027 active HSIN account holders external to DHS we surveyed identified challenges with HSIN's login process. Our survey of deactivated HSIN account holders external to DHS indicated similar concerns with the login process, with 392, or 34 percent, of 1,159[29] respondents identifying login issues as a reason they stopped using HSIN. More specifically, 246 deactivated respondents cited login issues as the sole reason they stopped using HSIN. A survey

[29] DHS OIG received 1,710 responses from deactivated HSIN account holders. 551 of the deactivated HSIN account holders claimed they still use HSIN. These 551 account holders may use HSIN with another username and email. The remaining 1,159 deactivated HSIN account holder respondents no longer use HSIN.

respondent from state government identified login difficulties as the primary complaint from users within their state.

Partners were often unable to login to HSIN using their password. For example, during a site visit at a fusion center we observed a state employee unable to log into HSIN with their password when trying to demonstrate HSIN use to the audit team. The audit team also experienced password issues several times during the audit when attempting to access HSIN. Troubleshooting login issues with HSIN can be cumbersome, adding to reasons users did not use or stopped using HSIN. Users sometimes had to call the helpdesk if they experienced a login issue. Also, the system did not remind users when passwords were set to expire.

> "I do not know of a single HSIN user that enjoys using the platform or that does not have issues with it in some significant way. It often feels like you are fighting against HSIN to do the simplest tasks." – Active Account Holder Survey Respondent

Partners reported difficulty maintaining HSIN accounts and passwords. In March 2022, the Office of the CIO attempted to simplify the login process using a HSIN user's personal identity verification card. Since many non-Federal partners do not use personal identity verification cards, this solution is not available to them. Personal identity verification can expire in the system while usernames and passwords still work, requiring users to call the HSIN helpdesk to fix the issue. Some users resorted to signing into HSIN as a guest, which limited access to useful information available only to registered account holders.

DHS Did Not Conduct Outreach to Support Partners' HSIN Mission Needs

According to the Office of the CIO, as of 2023 there were 12 mission advocates[30] strategically located around the country who worked directly with the HSIN user base to provide users with customer service, training, and operations support. The Office of the CIO had a working group to communicate with users and obtain additional feedback on HSIN. Yet, multiple fusion centers did not know who their mission advocate was or how to contact them. One fusion center noted they previously had a great relationship with their HSIN mission advocate but no longer knew whom to contact for support following the original advocate's departure. A deputy director at another fusion center said, "We have not met a HSIN mission advocate, and I am not sure the HSIN advocates even exist." Some external partners interviewed communicated with their mission advocates when needed, while others did not know their mission advocate or how to find a mission advocate for support.

[30] According to the Office of the CIO, mission advocates are now called stakeholder engagement specialists and are no longer fusion centers' primary support for HSIN.

DHS Did Not Always Share Information with Partners in a Timely Manner

Fusion centers are the primary contacts between the HSE, state and local leadership, and frontline personnel. Fusion center personnel we interviewed expressed the need to communicate and share information in real time. Yet the NOC did not always provide threat information timely to its partners, including fusion centers. OSA, which includes the NOC, provides timely, accurate, and coordinated reporting on significant and upcoming DHS operations and operational responses.

The NOC receives potential emerging threat information daily. Prior to sharing threat information with partners, the NOC must determine the accuracy and significance of information. Appendix C provides an overview of the NOC's information sharing process. These steps may result in the NOC distributing actionable threat information to its partners after partners received the same information from other sources. Personnel at one fusion center reported NOC-provided information was helpful, but they had often already received the same information from other sources, such as law enforcement partners. One key stakeholder noted information from the NOC was helpful, but they hoped to receive information faster to meet their reporting needs. This partner noted receiving a phone call from the NOC when an event is first unfolding would be more helpful. Many other state and local partners we interviewed noted receiving the same information from the media, internal analysts, or local governmental and other external partners contacts prior to receiving it from the NOC.

Although fusion center personnel received threat information from the NOC, they did not always find it actionable. Fusion center partners that detailed officers to the NOC were more satisfied with the amount and frequency of NOC-provided information than partners who did not. During a site visit to a fusion center not local to Washington, DC, the fusion center's director said information provided by the NOC was usually not useful because it was not detailed or timely. According to one fusion center director, oftentimes the same information had already been reported by the media.

The NOC must maintain its relationships with information sharing partners to ensure it receives and shares relevant information timely and broadly. At times, the NOC only receives threat information from a partner with the understanding the partner must grant permission before the NOC can share the information further. According to one OSA executive, "collaboration happens at the speed of trust," limiting how quickly the NOC can share threat information.

Conclusion

As threats, including terrorism, continue to increase, sharing timely, actionable threat information with DHS partners is crucial to national security. DHS spent more than $38 million on threat sharing technology from FYs 2021 to 2023 and plans to spend more than $26 million to

modernize HSIN between FYs 2023 and 2025. However, partners continued to share information via workarounds including emails, phone calls, and business messaging applications and relied on internally developed systems.

If DHS cannot effectively share emerging threat information with its partners, its partners may not respond timely and effectively to potential threats against the homeland, such as at upcoming election events and holiday parades, and for mass casualty incidents. One DHS partner emphasized if external partners are not engaged for threat information, the Government will fail to protect that sector. Also, limited DHS partner use of information sharing technologies potentially hindered DHS' ability to notify partners of emerging threats, in support of the Department's statutory mission. If DHS can improve its information sharing technologies and accessibility, it may increase partner access to, and awareness of, threat information.

Finally, if users are unaware of HSIN modernization efforts or do not see changes to HSIN because they do not regularly login, the funds spent on system upgrades may not significantly increase access to, and awareness of, critical threat information. Without an easy-to-use platform and increased outreach, users will continue to seek alternative sources of threat information other than HSIN. One fusion center's deputy director said if DHS does not update HSIN, that fusion center "will move away from using it." If DHS and its partners stop using HSIN and other DHS technologies, useful threat information may be overlooked. Consequently, partners may not have access to real-time incident reporting, which may result in national security concerns.

Recommendations

Recommendation 1: We recommend the Office of Homeland Security Situational Awareness Director and the Intelligence and Analysis Under Secretary, with the support of the DHS Chief Information Officer, establish a recurring process to coordinate internally and with external partners to identify needed Homeland Security Information Network functionality improvements and provide the DHS Chief Information Officer with Homeland Security Information Network improvement recommendations.

Recommendation 2: We recommend the DHS Chief Information Officer create and implement a plan for outreach with external partners to increase awareness of Homeland Security Information Network capabilities, such as trainings and updates, and available resources, including stakeholder engagement specialists, to fusion centers.

Recommendation 3: We recommend the DHS Chief Information Officer conduct a cost benefit analysis to evaluate partners' Homeland Security Information Network use versus cost to modernize and determine if modernization is the best solution for Homeland Security Information Network based on fiscal responsibility, mission objectives, and user feedback.

Recommendation 4: We recommend the Intelligence and Analysis Under Secretary, in coordination with Office of Homeland Security Situational Awareness Director, create and implement a plan of action to expand outreach to other stakeholders, such as fusion centers and external partners, to promote access to DHS technologies including the Virtual Situation Rroom and the common operating picture.

Management Comments and OIG Analysis

The Department provided written comments in response to a draft of this report. We reviewed the Department's comments, as well as technical comments received under separate cover, and made changes to the report, as appropriate. In the comments, the Department noted it remains committed to prioritizing HSIN modernization and strengthening its effective use with partners. DHS concurred with recommendations 1 and 2 and did not concur with recommendations 3 and 4. We have included a copy of the comments in their entirety in Appendix B. We consider recommendations 1 and 2 open and resolved, and recommendations 3 and 4 open and unresolved. A summary of DHS' responses and our analysis follows.

DHS' Response to Recommendation 1: Concur. DHS' Office of the CIO uses several mechanisms to communicate with partners, both internally and externally. DHS' Office of the CIO also leverages those partnerships, as appropriate, to identify user requirements and solicit feedback on system developments. In FY 2025, the Office of the CIO will institute standard quarterly meetings and listening sessions for mission users to gather feedback. Expected date of completion: September 30, 2025.

OIG Analysis: DHS provided a corrective action plan and expected date of completion to satisfy the intent of the recommendation. We consider this recommendation open and resolved until we receive documentation demonstrating the Office of the CIO hosts the meetings and listening sessions and analyzes feedback received to make improvements to HSIN.

DHS' Response to Recommendation 2: Concur. DHS' Office of the CIO maintains mission advocates/stakeholder engagement specialists for HSIN, who are responsible for outreach to partners. They also collect requirements, conduct support, provide engagement updates, and share best practices. The Office of the CIO is working on a HSIN stakeholder engagement strategy, which once complete, will increase awareness of HSIN capabilities and updates among partners. There will also be briefings provided to all 80 fusion centers. Expected date of completion: September 30, 2025.

OIG Analysis: DHS provided a corrective action plan and expected date of completion to satisfy the intent of the recommendation. We consider this recommendation open and resolved until

we receive documentation of the FY 2025 Engagement Strategy and observe the strategy is carried out.

DHS' Response to Recommendation 3: Non-concur. DHS' Office of the CIO conducted a benefit analysis in March 2022 to evaluate HSIN use versus HSIN modernization and determined HSIN modernization is the best solution when considering fiscal responsibility, mission objectives, and user feedback. DHS' Office of the CIO proposed nearly $27 million to improve HSIN technology, including to rebuild HSIN's underlying platform as a cloud-optimized solution, enhance HSIN's user interface, and expand mobile solutions. The Technology Modernization Board approved DHS Office of the CIO's nearly $27 million modernization proposal in June 2022. DHS' Office of the CIO maintains that implementing the DHS Office of Inspector General's recommendation to conduct a cost benefit analysis to evaluate partners' HSIN use versus cost to modernize would be redundant.

OIG Analysis: We do not consider DHS' actions responsive to the recommendation, which is open and unresolved. The Office of the CIO did not provide documentation to demonstrate that partners' total number of users and uses of HSIN compared to the cost to modernize was considered when deciding to update the platform. The Office of the CIO affirmed its decision to modernize HSIN based on its interviews with 236 users, which represents less than half of 1 percent of all active HSIN account holders. As noted in our report, only approximately 26,000 users used the system within a 6-month period during the audit scope. Many of these users noted significant concerns with HSIN and are seeking alternative platforms. These findings are consistent with previous DHS OIG reporting on HSIN. Based on the number of survey respondents and interviews with people seeking alternative solutions, the number of HSIN complaints shared with the audit team, and a modernization effort of nearly $27 million, the intent of the recommendation was for the Office of the CIO to reconsider these factors before continuing to invest funds in HSIN.

DHS' Response to Recommendation 4: Non-Concur. The Office of the CIO drafted a new HSIN Stakeholder Engagement Strategy for FY 2025 in August 2024, which will increase awareness of HSIN capabilities and updates with partners, including fusion centers. The Office of the CIO will continue to communicate with partners via its regular HSIN user group meetings and other regular meetings with partners. The Office of the CIO will work with I&A and OSA, as appropriate, to create and implement a plan to further expand outreach to HSIN, which will include communities of interest for the NOC's COP and vSITROOM. Expected date of completion: September 30, 2025.

OIG Analysis: We do not consider DHS' actions fully responsive to the recommendation, which is open and unresolved. While we agree with the steps the Office of the CIO plans to take, the recommendation was issued to I&A and OSA, which did not provide a formal response. The intent of this recommendation was for I&A and OSA to expand outreach with partners and fusion

centers as they are the Department's connection to fusion centers. As noted in our report, HSIN mission advocates were hard to locate and mission advocates (now stakeholder engagement specialists) are no longer fusion centers' primary support for HSIN. Although the Office of the CIO is HSIN's system owner, we also made this recommendation to I&A and OSA as they are the primary users of the COP and vSITROOM and are in a better position to promote those technologies with existing partners.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine whether DHS has technology to identify and share actionable information on emerging threats with its external partners. The scope of this audit includes DHS' efforts to identify and share information on emerging threats from March 2022 through February 2024.

During this audit, we researched and reviewed more than 150 Federal laws, departmental and component policies, procedures, prior reports, and component documents related to our objective.

We traveled to Washington, DC, to interview and observe OSA, the NOC, and their information sharing practices and technologies. We also interviewed I&A's Field Intelligence Directorate in Washington, DC. We interviewed the Office of the CIO regarding HSIN, including improvements and modernization efforts. We interviewed personnel from 11 fusion centers, including fusion center leadership, fusion center analysts, I&A intelligence officers, and other I&A staff to observe fusion centers' employed technologies used to analyze emerging threat information for external partners. In addition to fusion centers, we interviewed 16 external partners, including private sector partners, regarding information sharing technologies and practices. We attended one National Special Security Event in San Francisco to observe how DHS shares threat information during special events. Audit team members visited the event's coordination center in San Francisco and the NOC in Washington, DC, during the event to observe information sharing.

We assessed data reliability of HSIN account holder data, including account holder emails and login frequency and use by (1) performing electronic testing, (2) reviewing existing information about the data that produced it, and (3) interviewing agency officials and system users knowledgeable about the data. The audit team had direct access to HSIN during the audit and obtained data relevant to our objective. The total count of account holders obtained and analyzed from HSIN data was 219,804 as of September 2023.

The audit team developed two voluntary electronic surveys using a secure, web-based survey software to analyze HSIN account holders' survey responses to questions regarding HSIN use. All survey responses were anonymous, and we reported aggregated survey results.[31]

- The audit team sent a survey to 44,550 active HSIN account holders external to DHS to complete between January 8 and January 15, 2024. 1,027, or 2 percent, of the 44,550 active HSIN account holders responded.
- The audit team sent a survey to 127,331 deactivated HSIN account holders external to DHS to complete between January 29 and February 10, 2024. 1,710, or 1 percent, of the 127,331 deactivated account holders responded to the survey.

We assessed the design, implementation, and operating effectiveness of DHS' internal controls related to our audit objective. Based on our assessment, we determined the overall internal controls risk is moderate and identified weaknesses in the body of this report. Since our internal control assessment was limited to the audit objective, it may not have disclosed other internal control deficiencies that potentially existed at the time of this audit.

We conducted this audit from June 2023 through February 2024 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

During this audit, the Department provided timely responses to our requests for information and did not delay or deny access to information we requested.

[31] We conducted non-statistical surveys. The survey results presented throughout this report cannot be projected to the entire population of HSIN account holders. Our survey results are only representative of the views of the active and deactivated HSIN account holders external to DHS who responded to our survey.

Appendix B:
DHS Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

BY ELECTRONIC SUBMISSION

September 16, 2024

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

FROM: Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2024.09.16 13:36:42 -04'00'

SUBJECT: Management Response to Draft Report: "DHS Partners Did Not Always Use DHS Technology to Obtain Emerging Threat Information (Project No. 23-032-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition that DHS utilizes technology which enables identification and sharing of emerging threat information, including technological methods for maintaining real time situational awareness and identifying threat information, such as the Office of Homeland Security Situational Awareness' media monitoring and a virtual situation room. The Homeland Security Information Network (HSIN) application, that DHS utilizes to share this information, was accessed a total of 2,441,318 times during fiscal year (FY) 2023 which represents a significant volume of users—the majority of which access the platform for seasonal events each year (e.g., hurricanes, the Super Bowl, etc.).

DHS remains committed to prioritizing HSIN modernization and strengthening its effective use for the trusted sharing of Sensitive But Unclassified information:

- between federal, state, local, territorial, tribal, international and private sector partners, and
- among mission operators to access Homeland Security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions and help keep their communities safe.

Leadership, however, is concerned about OIG's inaccurate assertion the DHS Office of the Chief Information Officer (OCIO) delayed access to information OIG, which DHS believes is misleading to end users of OIG's report due to a lack of context regarding what actually happened. To be clear, as the OIG acknowledges, OCIO maintained consistent communication with the audit team throughout this entire audit that began more than a year ago in June 2023. However, out of twenty OIG requests for information, DHS is only aware of one instance occurring on March 18, 2024, in which OCIO provided six months of data instead of the 12 months requested due to system configuration setting that limited the availability of the data. OCIO ensured that OIG received timely and complete information for the 19 other requests for HSIN documents and information which included information on nearly 220,000 HSIN users (both active and inactive) spanning over several years.

The draft report contained four recommendations, two with which the Department concurs (Recommendations 1 and 2) and two with which the Department non-concurs (Recommendations 3 and 4). Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration, as appropriate.

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.

Attachment

Attachment: Management Response to Recommendations Contained in 23-032-AUD-OSA

OIG recommended that the Office of Homeland Security Situational Awareness (OSA) Director and the Office of Intelligence and Analysis (I&A) Under Secretary, with the support of the DHS Chief Information Officer (CIO):

Recommendation 1: Establish a recurring process to coordinate internally and with external partners to identify needed HSIN functionality improvements and provide the DHS Chief Information Officer with HSIN improvement recommendations.

Response: Concur. DHS OCIO uses several mechanisms already in place to communicate with internal and external partners, such as HSIN's Executive Steering Committee, led by the I&A CIO and OSA Deputy Director, which meets quarterly to discuss HSIN functionalities for all HSIN users across various missions and to solicit recommendations and guidance for the platform. HSIN personnel also meet weekly with DHS I&A to coordinate on system improvements and external engagement opportunities.

Further, DHS OCIO meets as needed with various internal and external partners including federal, state, local, tribal, territorial, international, and private partners, as appropriate, to identify user requirements, solicit feedback and inform on new system developments. During FY 2025, OCIO will also institute standard quarterly meetings and listening sessions for mission users, as well as continue to meet with international users on an "as needed" basis to gather user feedback. Estimated Completion Date (ECD): September 30, 2025.

OIG recommended that the DHS CIO:

Recommendation 2: Create and implement a plan for outreach with external partners to increase awareness of HSIN capabilities, such as trainings and updates, and available resources, including stakeholder engagement specialists, to fusion centers.

Response: Concur. OCIO, as the system owner for HSIN, agrees with the importance of stakeholder engagement and outreach initiatives with external partners. Accordingly, DHS maintains HSIN Mission Advocates/Stakeholder Engagement Specialists that are responsible for outreach with federal, state, local, tribal, territorial and private sectors stakeholders across the homeland security enterprise. Additionally, these Mission Advocates/Stakeholder Engagement Specialists collect requirements, conduct support for Communities of Interest (COI), and provide engagement for updates, best practices. Further, in August 2024, OCIO outlined an initial draft of a new HSIN Stakeholder Engagement Strategy for FY 2025 which, once complete, will increase awareness of HSIN capabilities and updates among external partners, such as through briefings to all

80 fusion centers in FY 2025. OCIO will also continue its practice of hosting HSIN User Group (HUG) webinars, typically attended by 300-500 users, which highlight HSIN's mission critical use, future modernization capabilities, and available resources. In FY 2023, OCIO hosted nine HUGs, and six HUGs thus far in FY 2024. ECD: September 30, 2025.

Recommendation 3: Conduct a cost benefit analysis to evaluate partners' HSIN use versus cost to modernize and determine if modernization is the best solution for HSIN based on fiscal responsibility, mission objectives, and user feedback.

Response: Non-Concur. In March 2022, DHS OCIO conducted a modernization benefit analysis evaluating HSIN use versus HSIN modernization, and determined HSIN modernization is the best solution when factoring in fiscal responsibility, mission objectives, and user feedback. The analysis yielded the disbursement of $26.9 million from the Technology Modernization Funding (TMF) between FY 2022 - FY 2024 for system platform development, which initiated modernization in FY 2022 that is currently underway.

Specifically, DHS proposed $26.95 million for the following technology improvements: (1) Rebuild the underlying HSIN platform as a cloud-optimized solution, capable of scaling to meet demand; (2) Enhance HSIN user interface to improve search capabilities and visual analytics for sensitive but unclassified information; and (3) Expand mobile solutions for state and local partners with certified credentials. Further, when considering the 236 user interviews OCIO conducted on modernization during FY 2022 - FY 2023, the HSIN modernization initiative is affirmed as the best solution for HSIN based on fiscal responsibility, mission objectives, and user feedback.

It is also important to note that the independent Technology Modernization Board[1]—comprised of senior government officials and chaired by the Federal CIO—reviewed and approved the Department's TMF proposal on June 21, 2022, determining that the Department's business case for the HSIN modernization effort exceeded the threshold required for TMF funding. The Department's current HSIN modernization effort, leveraging the approved TMF funding, is well beyond the point at which any additional alternative cost benefit analysis would be worthwhile. To the contrary, such an analysis would be redundant and may undermine current HSIN modernization efforts by unnecessarily diverting critical program resources.

We request that the OIG consider this recommendation resolved and closed, as implemented.

[1] https://tmf.cio.gov/board/

OIG recommended that the I&A Under Secretary, in coordination with OSA Director:

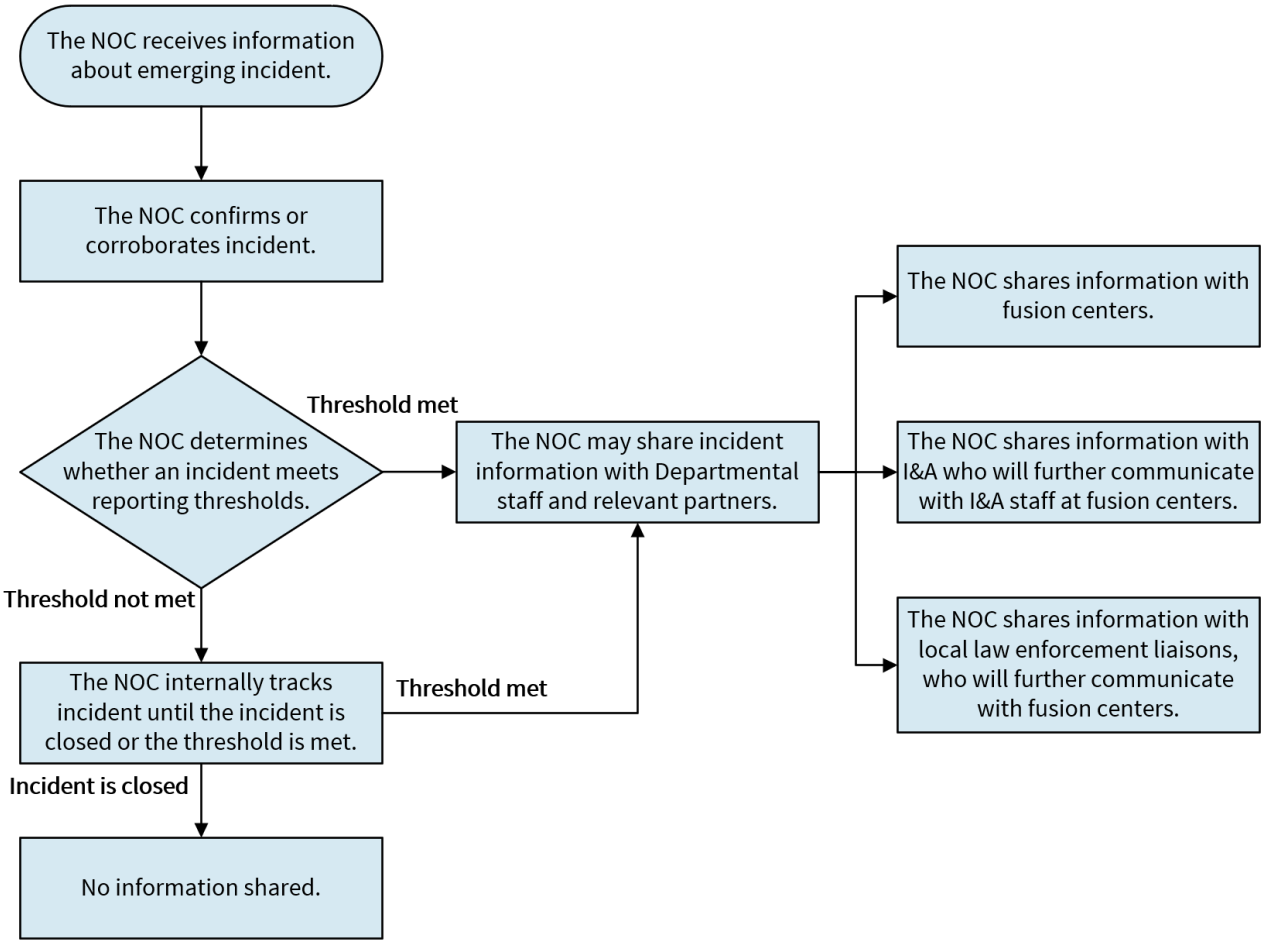
Recommendation 4: Create and implement a plan of action to expand outreach to other stakeholders, such as fusion centers and external partners, to promote access to DHS technologies including the Virtual Situation Room and the Common Operating Picture.

Response: Non-Concur. OCIO as the system owner for HSIN, agrees with the importance of stakeholder engagement and outreach initiatives with external partners. DHS OCIO accordingly maintains HSIN Mission Advocates/Stakeholder Engagement Specialists responsible for outreach with stakeholders across the homeland security enterprise and collects requirements, conducts support for COIs, and provides engagement for updates, best practices. Further, OCIO: (1) outlined an initial draft of a new HSIN Stakeholder Engagement Strategy for FY 2025 in August 2024, which will increase awareness of HSIN capabilities and updates among external partners, such as through briefings to all 80 fusion centers during FY 2025; (2) will continue its practice of hosting HUG webinars typically attended by 300-500 users, which highlight HSIN's mission critical use, future modernization capabilities, and available resources (e.g., in FY 2023, OCIO hosted nine HUGs and has conducted six thus far in FY 2024); and (3) will continue to use several mechanisms already in place to communicate with internal and external partners, including HSIN's ESC) led by the I&A CIO and OSA Deputy Director and which meets quarterly to discuss HSIN functionalities for all HSIN users across various missions and to solicit recommendations and guidance for the platform. HSIN personnel will also continue to meet weekly with DHS I&A to coordinate on system improvements and external engagement opportunities.

To reiterate, the OCIO meets as needed with various internal and external partners including federal, state, local, tribal, territorial, international, and private partners, as appropriate, to identify user requirements, solicit feedback, and inform on new system developments. In addition, the OCIO will institute standard quarterly meetings and listening sessions for mission users during FY 2025, while continuing to meet with international users on an "as needed" basis to gather user feedback. OCIO will also work with I&A and OSA, as appropriate, to create and implement a plan to further expand outreach to HSIN. This will include a Common Operating Picture COI and Virtual Situation Room COI. ECD: September 30, 2025.

5

Appendix C:
Overview of the NOC's Information Sharing Process



Source: DHS OIG-created based on NOC data[32]

[32] Appendix C does not account for all information sharing processes and does not include information that fusion centers and other partners may share back to the NOC. The NOC shares information in accordance with the handling constraints placed on the information by the originator of the information.

Appendix D:
DHS OIG Survey Results

Survey Type	Category	Count
Deactivated Account Holder Survey:	Surveys emailed to non-DHS deactivated account emails	127,331
	Deactivated account survey responses	1,710
Active Account Holder Survey:	Surveys emailed to non-DHS active account emails	44,550
	Active account survey responses	1,027

1. **Survey results from DHS OIG's survey of non-DHS deactivated HSIN account holders:**

   Why did you stop using DHS' HSIN?

Respondent Options	Respondents
Login Issues	392
Not user friendly	290
Lack of HSIN training	163
Information is not timely	61
Lack of HSIN support	59
Information is not accurate	24
Total Responses	**989**[33]

[33] 1,710 deactivated HSIN account holders external to DHS responded to this DHS OIG survey. Some respondents claimed they still use HSIN and others did not specify why they stopped using HSIN. The total of 989 responses represents the respondents who no longer use HSIN and selected one or multiple options.

2. **Survey results from DHS OIG's survey of non-DHS active HSIN account holders:**

How often do you use HSIN?

Respondent Options	Respondents
Daily	114
Weekly	254
Monthly	273
Less than monthly	306
I do not use HSIN	80
Total Responses	**1,027**

What sector is your HSIN account associated with?

Respondent Options	Respondents
State, Local, Territorial, or Tribal	568
Federal Government	279
Private	109
International	24
Other	47
Total Responses	**1,027**

Does HSIN have challenges in any of the below areas?

Respondent Options	Respondents
Ease of use	447
Login Process	371
HSIN does not have any challenges	302
HSIN registration process	180
Sharing Information	168
Helpdesk Communication	88
Total Responses	**1,556**[34]

[34] 1,027 active HSIN account holders external to DHS responded to this DHS OIG survey. Respondents were able to select multiple options for this question. Therefore, the total response sum to more than 1,027.

Have you heard of a HSIN modernization effort?

Respondent Options	Respondents
Yes	206
No	821
Total Responses	**1,027**

Are you aware of training for HSIN?

Respondent Options		Respondents
Yes, and:	I have not taken HSIN training	326
	I have taken HSIN training and it was helpful	232
	I have taken HSIN training but it was not helpful	34
No		435
Total Responses		**1,027**

Source: DHS OIG analysis of survey results

Appendix E:
Report Distribution

Department of Homeland Security

Secretary
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
Chief Information Officer, The Office of the CIO
Director, OSA
Under Secretary, I&A
The Office of the CIO Liaison
OSA Liaison
I&A Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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