Agenda

June 23, 2026
Antigua 3
Caribe Royal Hotel
Orlando, FL

7:30	Registration Opens (Palms Atrium) Please check in for the ISAC Annual Meeting
7:30—8:30	Continental Breakfast (Grand Sierra D/E) Breakfast is provided as part of the ISAC Annual Meeting
8:45—9:00	Opening Remarks & Day 1 Recap (Palms 1/2) This opening session of the day is available to all NHSC participants.
9:00—10:00	(ISAC Annual Meeting) Keynote Presentation – Cyberchat: Insights for Elevating Cyber Resilience in Your Organization (Palms 1/2) This keynote is available to all NHSC participants. Chris Tarbell, Director, Cyber Security and Investigations, Berkley Research Group and Former FBI Special Agent Hector Monsegur, Cyber Security Expert and Co-founder, SafeHill Once adversaries in the cybersphere, Hector Monsegur and Chris Tarbell have joined forces to help organizations confront today's most pressing cyber threats. Drawing on their extraordinary experiences - one as a former black-hat hacker, the other as an FBI special agent - their conversation offers a rare, dual-lens view of the modern threat landscape. In a dynamic, audience-driven discussion, Monsegur and Tarbell break down the most significant risks facing organizations today, how real-world attacks unfold, and where defenses most often fail. Together, they share practical insights and actionable frameworks that leaders can apply to strengthen security, reduce risk, and protect operations from disruptions that can cripple organizations and erode trust.

[NHSC Meeting Begins in Antigua 3]

10:00—10:15	Welcome and Introductions (Antigua 3) Tri-Chairs: A.J. Schall (NEMA) and Mark Sloan (BCEM)
10:15—11:00	Inventory of Current Events Since Last Meeting Homeland security remains a dynamic subject matter since the last meeting of the NHSC. We will spend some time inventorying the current concerns being addressed by associations. This round-robin format will be facilitated by the NHSC Tri-Chairs.
11:00—11:45	Discussion of FEMA Review Council Actions In May of this year, the FEMA Review Council established by executive order released their long-awaited report on proposed FEMA reforms. The NHSC Tri-Chairs will walk through the

recommendations and participants can discuss impacts, concerns, and advocacy actions for each discipline represented.

11:45—12:10 Break

12:10—1:10 September 11 and Lessons Learned Over 25 Years
Mike Little, IAFC

With the 25th anniversary of September 11 occurring in just three months, this retrospective presentation will take a look at where we stand as a nation over the past quarter century. Chief Little will walk through lessons learned, remaining obstacles, and how the events of that day forever shaped our current profession.

1:10—1:35 Lunch (Palms 1/2)
Lunch is provided as part of the ISAC Annual Meeting

1:35—2:30 Discussion with Center for Internet Security (CIS)
John Gilligan, President & CEO

The Multi-State Information Sharing and Analysis Center (MS-ISAC), operated by the independent, nonprofit Center for Internet Security, was first established in 2003 to serve as the nation's primary collaborative entity for protecting state, local, tribal, and territorial governments from cyberattacks. As the federal government shifts its approach on cybersecurity, the state-local partnership is more important than ever. Complicating this new environment is that cyberattacks are shifting from espionage and data theft toward physical disruption of our critical infrastructure. How do we prepare to protect our communities in this changing landscape? CIS officials will provide some background and seek input from NHSC members.

2:30—3:30 Threats to Large-Scale Events: Future Planning Considerations
Kevin Saupp, Center for Internet Security

Building on the extensive planning and operational efforts associated with the World Cup, this session will provide an opportunity to assess lessons learned, identify emerging challenges, and discuss future priorities for securing large-scale events. The discussion will examine what worked, where gaps remain, and how the threat landscape continues to evolve across both physical and digital domains — including unmanned aircraft systems (UAS), cyber threats, synthetic media/deepfakes, ticketing and access platforms, and other emerging risks. Participants will share perspectives from World Cup planning and operations, with a focus on identifying key considerations, capability gaps, and opportunities to inform future priorities, planning efforts, and recommendations for federal, state, local, tribal, and territorial partners.

3:30—4:00 Next Steps for the NHSC

4:00 Adjourn

Discussion Summary

June 23, 2026
Orlando, FL

A meeting of the National Homeland Security Consortium (NHSC) was held on June 23, 2026, in Orlando, Florida. This document briefly summarizes the meeting's discussions.

Inventory of Current Events Since Last Meeting (Roundtable Discussion)

Tri-Chairs A.J. Schall and Mark Sloan kicked off the meeting by facilitating a roundtable discussion among the participants on their current priorities, concerns, and challenges. The meeting highlighted widespread concern about ongoing federal funding reductions, uncertainty surrounding the Federal Emergency Management Agency (FEMA) and Department of Homeland Security (DHS) reforms, and the difficulty state and local agencies face in planning for the future without clear guidance, predictable funding streams, or a defined federal role. Participants repeatedly emphasized that states and local governments are increasingly being forced to identify alternative funding sources, build new partnerships, and prepare to assume greater responsibility for homeland security and emergency management activities.

Much of the discussion focused on the operational impacts of federal policy changes and emerging threats. Representatives from emergency management, public health, fusion centers, EMS, and cybersecurity organizations described staffing reductions, grant uncertainty, delayed funding cycles, and diminished federal support for information sharing, training, and preparedness programs. At the same time, participants noted that threat levels continue to grow and evolve, including concerns related to nation-state activity, terrorism, cyber threats, artificial intelligence (AI), critical infrastructure vulnerabilities, public health threats, and major events such as the ongoing FIFA World Cup. Several participants emphasized that while federal support remains important, state and local governments can no longer assume the federal government will serve as a consistent/reliable partner and must increasingly build their own capabilities and capacity.

Despite the challenges discussed, participants also highlighted several positive developments and opportunities. There was broad recognition of the value of interstate and cross-sector collaboration, including efforts through the Emergency Management Assistance Compact (EMAC), cybersecurity information-sharing organizations, and partnerships among state and local agencies. Many participants emphasized the need for greater integration across emergency management, homeland security, public health, law enforcement, cybersecurity, and critical infrastructure communities to address increasingly interconnected threats.

Discussion of FEMA Review Council Actions (Roundtable Discussion)

The meeting then transitioned to a discussion of the recently released FEMA Review Council (FRC) report and its recommendations for the future role of FEMA, state governments, and local jurisdictions in emergency management. Participants generally agreed with the report's broad goals (e.g., strengthening state and local leadership in disaster response, accelerating federal assistance, increasing transparency, streamlining programs) but expressed significant concern about many of the specifics and the lack of clarity regarding implementation.

Several participants noted that while the vision is appealing at a high level, many of the recommendations require legislative or regulatory action, making meaningful changes unlikely in the near term given the current political environment. There was a recurring theme that states and local governments need more certainty, funding guidance, and lead time to adapt their programs, budgets, and staffing if federal responsibilities are devolved to the states.

A substantial portion of the roundtable discussion centered on disaster assistance timelines, funding responsibilities, and FEMA's future structure. Participants highlighted ongoing frustrations with the lengthy federal declaration process and Individual Assistance (IA) approval processes, noting that communities often need help long before federal aid becomes available. While there was support for making FEMA more efficient, participants questioned what a "leaner" FEMA would mean in practice, particularly given recent staff reductions and the loss of institutional expertise. Others emphasized the need for a broader national conversation about the fundamental purpose of programs such as Public Assistance (PA), IA, Hazard Mitigation Grant Program (HMGP), and the National Flood Insurance Program (NFIP) before meaningful reform can occur.

Despite concerns with certain FRC recommendations, several participants shared positive recent experiences with FEMA coordination and praised the Small Business Administration (SBA) for its responsiveness and outreach efforts. The discussion ended with a recognition that major policy changes are likely to occur slowly, and that continued collaboration among federal, state, local, and territorial partners (through forums like the NHSC) will be essential as the disaster management landscape evolves.

September 11 and Lessons Learned Over 25 Years

- ***Mike Little, International Association of Fire Chiefs***

Mike Little then transitioned to a presentation on the September 11 attacks and the lessons the nation has learned in the subsequent 25 years. Little emphasized that 9/11 was a transformative event that fundamentally reshaped national security, emergency management, intelligence sharing, and public awareness. Beyond the nearly 3,000 lives lost on the day of the attacks, the discussion highlighted the broader human toll, including military casualties from post-9/11 conflicts, long-term health impacts on responders, and the continuing effects on families and their communities. Little noted that many of the organizations, policies, and frameworks that exist today (e.g., DHS, fusion centers, intelligence-sharing mechanisms, and public initiatives such as "See Something, Say Something") were created or significantly expanded in response to lessons learned from 9/11.

A significant portion of Little's presentation focused on the changing threat environment and whether current preparedness efforts remain aligned with emerging risks. While he acknowledged that jihadist terrorism remains a concern, Little noted that the threat landscape has expanded to include domestic violent extremism, active shooters, ideologically motivated violence, and more. Participants expressed concern that the homeland security community may be drifting back toward "organizational silos," potentially weakening the collaboration that became so important in the post-9/11 era.

Particular attention was given to intelligence sharing, with participants noting the value of fusion centers while also discussing ongoing challenges related to dissemination, information accessibility, and ensuring that non-traditional partners (e.g., public works, fire services, and other community stakeholders) receive information in a timely manner. There was broad agreement that effective prevention and response depend on maintaining strong partnerships across federal, state, local, tribal, and private-sector organizations.

The session concluded with a forward-looking discussion about sustaining the capabilities and relationships built since 9/11. Participants identified continued investment in interoperability, EM frameworks, active-threat preparedness, intelligence analysis, and emerging technologies such as artificial intelligence as important priorities. At the same time, they cautioned against complacency, warning that a loss of vigilance and institutional memory could erode many of the gains achieved over the past two decades. Little emphasized that the legacy of 9/11 should not be viewed solely as a historical event, but as an ongoing reminder of the need for preparedness, information sharing, resilience, and whole-community engagement in addressing security challenges.

Discussion with Center for Internet Security

- ***John Gilligan, Center for Internet Security***

John Gilligan then provided a briefing focused on the evolving cybersecurity landscape and the role of the Center for Internet Security (CIS) in helping SLTT governments strengthen their cyber resilience. Gilligan provided an overview of CIS's mission, highlighting its long-standing work developing cybersecurity best practices, including the CIS Benchmarks and Critical Security Controls. Gilligan emphasized the importance of prioritizing foundational "cyber hygiene" measures, noting that implementation of core security controls can mitigate the vast majority of the most common cyber threats. Gilligan also discussed broader efforts around Secure-By-Design software development, reasonable security standards, and community-wide cybersecurity initiatives that extend beyond government agencies to include private-sector partners and residents. Lessons learned from a pilot "Secure Cyber Cities" initiative underscored that organizational culture, leadership engagement, and cross-sector collaboration are often more challenging than the technical aspects of cybersecurity efforts.

Gilligan also reviewed emerging threats and trends affecting government organizations. AI was described as both a growing risk and a valuable tool, with Gilligan noting that AI-generated attacks, "deepfakes," surveillance technologies, and increasingly sophisticated adversaries are reshaping the threat environment. At the same time, AI is being incorporated into defensive cybersecurity capabilities, vulnerability identification, and threat analysis. Gilligan highlighted ongoing support for major events such as the FIFA World Cup and preparations for upcoming elections, emphasizing the need for an all-hazards approach that integrates cybersecurity, law enforcement, emergency management, and critical infrastructure protection. Concerns were raised about declining federal cybersecurity support and the growing responsibility being placed on state and local governments to protect systems that underpin national and economic security.

Additionally, a significant portion of the conversation focused on the Multi-State Information Sharing and Analysis Center (MS-ISAC) and its transition from a federally funded model to a membership-based structure following the loss of federal grant support. Gilligan acknowledged that the transition has created challenges but stressed CIS's commitment to maintaining cybersecurity services for SLTT entities. He emphasized the value of MS-ISAC's nationwide threat intelligence sharing, security operations center capabilities, and partnerships with industry leaders. The discussion highlighted the difficulty many states face due to fragmented authorities, funding constraints, and limited coordination among CIOs, CISOs, homeland security offices, and local governments. Participants agreed that stronger statewide collaboration, broader awareness of available resources, and a "whole-of-state" approach are essential to protecting organizations and critical infrastructure from increasingly complex cyber threats.

Threats to Large-Scale Events: Future Planning

- ***Kevin Saupp, Center for Internet Security***

Kevin Saupp then delivered a briefing on planning for threats to large-scale events. The discussion focused on the evolving threat environment surrounding major special events, with emphasis on security planning and intelligence support for the FIFA World Cup and future large-scale events. Saupp highlighted the unprecedented scale and complexity of the World Cup, involving multiple countries, venues, transportation systems, and stakeholders. He emphasized that the security landscape has expanded beyond traditional physical threats to include digital and physical risks such as cyberattacks, drone activity, "deepfakes," foreign influence operations, and threat actors employing AI. These emerging technologies are creating new challenges for public safety agencies and event organizers, requiring continuous adaptation of planning assumptions, risk assessments, and response capabilities.

A significant portion of the discussion focused on information sharing and situational awareness. Participants cited examples where timely intelligence sharing helped identify potential threats and improve operational awareness. The discussion also emphasized the importance of cross-sector collaboration among law enforcement, fusion centers, emergency management, homeland security, public works, public health agencies, and private-sector partners.

Looking ahead, Saupp stressed the need to apply lessons learned from current World Cup operations to future large-scale events, including the 2028 Olympics, the 2031 FIFA Women's World Cup, and the 2034 Winter Olympics. Key areas of concern included counter-drone capabilities, airspace management, cyber resilience, digital ticketing security, public health surveillance, and the impact of AI-generated misinformation. The briefing emphasized that future success will depend on sustained investment in technology, interoperable information-sharing systems, workforce training, and stronger coordination mechanisms that include all relevant stakeholders, including those often overlooked.

National Homeland Security Consortium
Attendee List
Orlando, FL
June 23, 2026

American Public Works Association
Michael Millette
Director of Public Works
Village of South Elgin
mmillette@southelgin.com

Marty Williams
Sr. Government Affairs Manager
American Public Works Association
mwilliams@apwa.org

Association of State and Territorial Health Officials
Winfred Rawls
Association of State and Territorial Health Officials
wrawls@astho.org

Big City Emergency Managers
Ron Prater
Executive Director
Big City Emergency Managers
rprater@bigcityem.org

Mark Sloan
EMC
Harris County
mark.sloan@harriscountytx.gov

Governors' Homeland Security Advisors Council
A.J. Gary
Director and State Homeland Security Advisor
State of Arkansas
aj.gary@adem.arkansas.gov

National Association of County & City Health Officials
Jerry Joseph
Director of Preparedness
NACCHO
jjoseph@naccho.org

International Association of Emergency Managers
Thad Huguley
Director, Govt Affairs
IAEM
thad@huguleyconsulting.com

International Association of Fire Chiefs
Michael Little
Senior Intelligence Officer
Joint Regional Intelligence Center
mlittle@jric.org

International City/County Management Association
Sean McGlynn
City Manager
City of Escondido
sean.mcglynn@escondido.gov

Amber Snowden
Public Policy & Special Projects Advisor
ICMA
asnowden@icma.org

Major County Sheriffs' Association
Megan Noland
Executive Director
Major County Sheriffs of America
mnoland@mcsheriffs.com

National Association of Counties
Brett Mattson
Senior Legislative Director
NACo
bmattson@naco.o

National Homeland Security Consortium
Attendee List
Orlando, FL
June 23, 2026

National Association of State Emergency Medical Services Officials
Jonah Raether
Planning and Program Specialist
Rhode Island Department of Health
jonah.raether@health.ri.gov

National Emergency Management Association
Matt Cowles
Deputy Director
National Emergency Management Association
mcowles@csg.org

AJ Schall
Director
Delaware Emergency Managmeent Agency
a.j.schall@delaware.gov

Matt Shade
Policy Analyst
National Emergency Management Association
mshade@csg.org

Patrick Sheehan
Director
Tennessee Emergency Management Agency
patrick.sheehan@tn.gov

Trina Sheets
Executive Director
National Emergency Management Association
tsheets@csg.org

National Fusion Center Association
Mike Sena
Director - NCRIC/HIDTA & President - NFCA
NCRIC/HIDTA - NFCA
msena@ncric.ca.gov

National Governors' Association
Jessica Davenport
Program Director, Homeland Security & Cybersecurity
National Governors' Association
jdavenport@nga.org

Naval Postgraduate School Center for Homeland Defense & Security
Dawn Wilson
Director-Executive Education Program
Naval Postgraduate School Center for Homeland Defense & Security
ndwilson@nps.edu

Speakers
Brian deVallance
Policy & Outreach
CIS
brian.devallance@cissecurity.org

John Gilligan
President & CEO
Center for Internet Security (CIS)
john.gilligan@cissecurity.org

Rich Neely
Executive Vice President & General Manager
CIS
rich.neely@cissecurity.org

Kevin Saupp
Senior Advisor
CIS
kevin.saupp@cissecurity.org

The President's Council to Assess the Federal Emergency Management Agency

Final Report Overview

Discussion Points

- The Council's Task
- Guiding Principles
- Listening to the Nation
- Key Recommendations
- Looking Forward

The Council's Task: Executive Order 14180

President Donald J. Trump appointed ten Council members with two Co-Chairs, Secretary Mullin and Secretary Hegseth, to conduct a full-scale review to recommend to the President improvements or structural changes to promote the national interest and enable national resilience.

- Advise…on the existing ability of FEMA to capably and impartially address disasters
- A comparison of the FEMA responses with State, Local, and private sector responses
- Traditional role of States and their coordination with the Federal Government
- Shall advise the President on all recommended changes related to FEMA to best serve the national interest
- An account of the commentary and debate about the role and operation of FEMA in our Federal system
- An evaluation of whether FEMA can serve its functions as a support agency, providing supplemental Federal Assistance
- Assessment of the adequacy of FEMA's response to disasters during previous 4 years, including sufficiency of staffing
- Historical background of other periods in the Nation's history…methods by which disaster aid and relief were then provided
- Other recommended improvements to FEMA in the current statutory structure

On January 24, 2025, President Donald J. Trump established the Federal Emergency Management Agency Review Council (FEMA Review Council) through Executive Order 14180, *Council to Assess the Federal Emergency Management Agency*.

Listening to the Nation

In order to meet the mandate established by the President, for over a year the Council was deliberate in its actions, devoting significant time to engage across jurisdictional levels and with various entities to hear about their experiences with FEMA during and after disasters.

11,708
Public comments received and considered by the Council

1,387
Nationwide survey respondents that represented emergency management stakeholders across SLTT and non-governmental partners

16
In-person and virtual listening sessions that engaged all 50 states, as well as local, tribal, and territorial stakeholders

This robust engagement process has provided the Council with invaluable insights into the challenges and opportunities facing FEMA's operations. The feedback serves as a cornerstone for shaping the future of FEMA's programs, ensuring that reforms are informed by the lived experiences of those directly impacted by disasters and those responsible for managing emergency response and recovery efforts.

Guiding Principles

After an exhaustive national review of the nation's ability to prepare for, respond to, and recover from natural disasters, the Council developed five guiding principles for reform:

Council Guiding Principles

- **Return** leadership for emergency response and recovery to the States, Tribes, and Territories
- **Reaffirm** that individual American preparedness is foundational to disaster readiness
- **Accelerate** federal assistance dollars to help Americans **recover from their worst day**
- **Maximize** the transparency and efficiency of federal and SLTT dollars spent in emergency management
- **Boldly transform** FEMA into a lean organization that puts **Americans first**

Key Recommendations

With the aforementioned guiding principles as a framework, the Council's report provides ten key recommendations that will boldly transform FEMA as an agency as well as address the return of leadership and responsibility for disaster management to the States, Local Communities, Tribes, and Territories.

1. Equip SLTT to lead disaster response with the federal government in a supporting role
2. Enhance critical federal programs & resources to support communities
3. Realign the criteria for federal disaster assistance
4. Replace the Hazard Mitigation Grant Program with a two-phase funding structure
5. Streamline the Individual Assistance program into a single direct payment program
6. Reform the Public Assistance program to provide direct funding
7. Reform the National Flood Insurance Program for financial stability and risk resilience
8. Maximize every dollar spent by reducing administrative costs
9. Revitalize A Unified National Network for Partnership
10. A Transformed Agency

Equip SLTT to Lead Disaster Response with the Federal Government in a Supporting Role

Reorienting the National Preparedness System to empower SLTT governments to manage the mitigation, response, and recovery of disasters effectively will return the federal role from leading to supporting.

Lack of a national standard for incident response and recovery

- Encourage adoption of national capability standards
- Incentivize building scalable training resources
- Professionalize emergency management to promote professional development
- Focus on catastrophic planning and promote a common approach to exercise standards

Limited ability to share and coordinate resources

- Revitalize and promote the use of the Unified Resource Catalog
- Refocus SLTT grant investment on mission-ready teams, capabilities, and infrastructure
- Enhance and improve upon the existing credentialing framework
- Promote the integration of additional partners including volunteer/faith-based
- Incentivize investments in interoperable systems for communication and data sharing

A truly resilient nation depends on seamless collaboration across government, private industry, and nonprofit partners. Empowering SLTT governments to take the lead in managing disasters is essential for a resilient national preparedness strategy.

Enhance Critical Federal Programs & Resources to Support Communities

The Council recommends that the future agency preserve and modernize the federal government's capability to support state and local partners in lifesaving and life-sustaining efforts.

- Sustain Core Standards to support effective and interoperable teams
- Integrate Emerging Technology
- Improve Federal Coordination
- Leverage Supply Chains for National Security
- Build Capacity for Emerging Threats
- Continuity of Government

The agency maintains an arsenal of dual-use capabilities, regional offices, incident management teams, and prepositioned logistic systems or programs, and the Disaster Relief Fund to ensure the American people are resilient in the face of any threat, whether natural or man-made. Therefore, sustaining and resourcing this mission in the transformed agency is vital to public safety, economic stability, and national resilience.

Realign the Criteria for Federal Disaster Assistance

Federal assistance should only be reserved for truly significant events that exceed SLTT capacity and capability. Therefore, common criteria should be established on how to evaluate when this occurs. This includes a reset of the Per Capita Indicator (PCI) threshold using the Consumer Price Index to account for historical inflation. The current disaster declarations process for federal assistance does not adequately account for SLTT capacity and, therefore, is inconsistent with legislative intent and disincentivizes SLTT investment in disaster preparedness.

Reassess

Review existing methodologies to realign criteria to reduce federal disaster declarations, leading to a rebalancing of state and federal responsibilities

Simplify

Eliminate the cost-to-capacity ratio and replace with an evaluation based on targeted factors like primary residence damage and other community impacts

Transparent

Utilize clear methodologies that help Americans easily understand federal responsibilities

The transformed agency should implement common-sense approaches to realign criteria for federal disaster declaration thresholds to return responsibility to the States, Tribes, and Territories.

Replace the Hazard Mitigation Grant Program with a Two-Phase Funding Structure

The Council proposes a state-managed program where project priorities are nationally set and environmental reviews are handled locally, with two phases of funding.

Rapid Mitigation

Within the first 30 days provide up to 5% of the federal government contribution for the disaster to facilitate immediate residential mitigation to primary residences and communities impacted by the event or in other high-risk zones

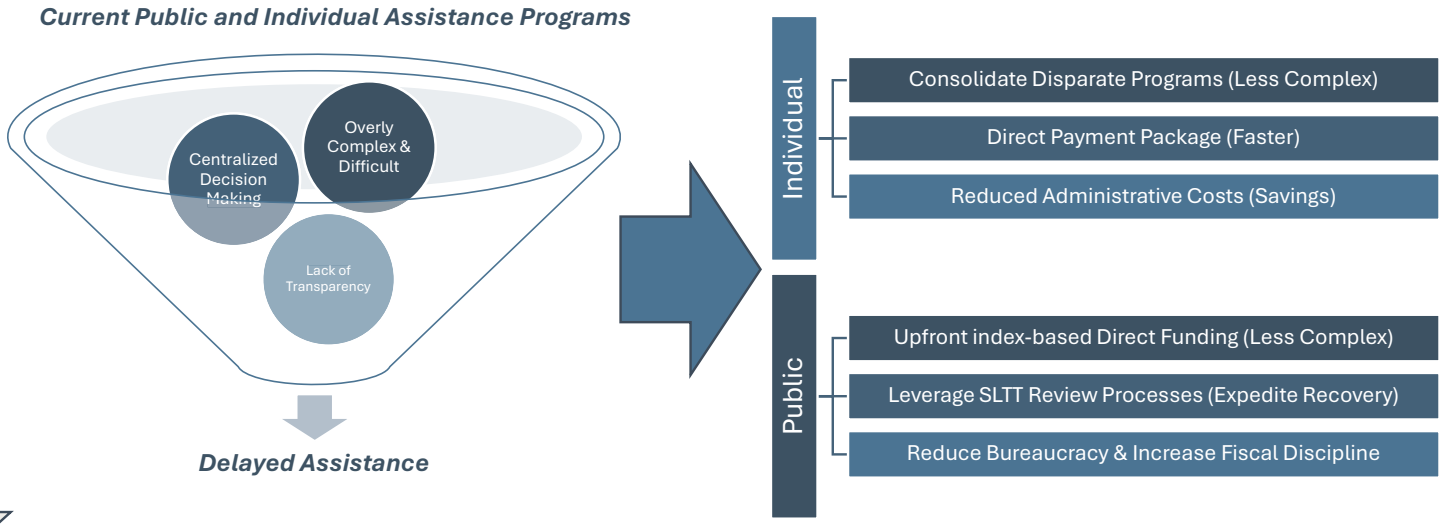
Strategic Mitigation

Within the first six months provide up to the remaining 10% of the federal government contribution to improve the performance of the NFIP by mitigating properties and critical infrastructure based on Federal Administration priorities

For mitigation to work, the Council recommends states take on greater program management responsibility and continue to develop an improved and comprehensive state hazard mitigation process that identifies projects that are immediately implementable.

Accelerating Federal Assistance

The transformed agency must accelerate federal assistance dollars to help Americans recover from their worst day.



By moving beyond slow and reactive traditional assistance programs, the new programs leverage flat-rate reimbursements for individuals, SLTT autonomy, near-immediate funding, and transparent auditing to reduce bureaucracy while creating faster, more effective, and more accountable systems for all Americans which will also remove FEMA from long-term recovery burdens.

Streamline the Individual Assistance Program into a Single Direct Payment Program

Swift support for emergency sheltering with a faster amount of monetary assistance would directly and positively impact affected Americans. Consolidating assistance into a single payment would provide all Americans clear, specific information on what assistance they would receive from the federal government in the event of a catastrophic loss.

Single Payment

Consolidate existing programs into one direct payment to survivors whose homes are uninhabitable after a disaster.

Focus on Emergency Housing

Focus the future agency's role on emergency and temporary housing (mass care/sheltering and temporary housing/rental assistance) instead of long-term housing, and only for Americans whose homes are uninhabitable (not those who experience minor damage).

These reforms will provide quick, cost-effective, and transparent support to disaster survivors, within the limits of federal funding, as well as reduce administrative overhead and clarify federal agency responsibilities. Further, there should be an option for this to be a state-managed program if individual states wish to do so.

Reform the Public Assistance Program to Provide Direct Funding

The Council proposes a modern and agile framework that converts the existing PA program into a direct funding model that leverages pre-defined objective event criteria and cost estimates to accelerate and streamline recovery.

Parametric Threshold

Utilizing a parametric threshold, funding would be released to states within 30 days of a major federal disaster declaration. This eliminates the need for time consuming loss assessments and quickly provides a financial backstop and cashflow for rapid response and recovery.

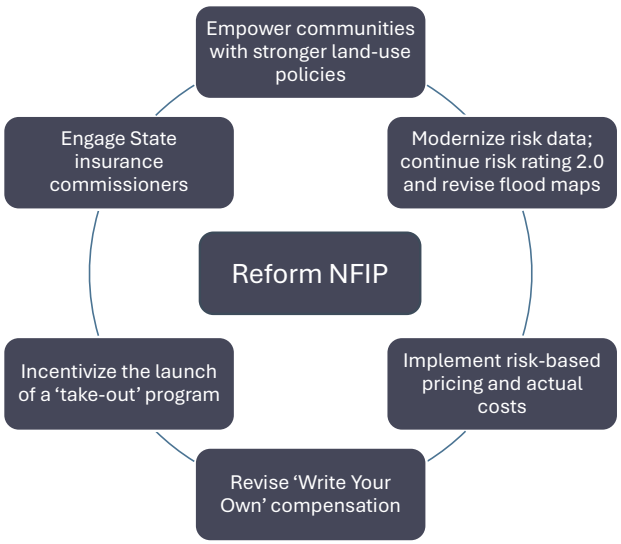
Accountability

Accountability would be maintained through a two-phase audit process: a one-time validation of costs within one year and a final program closeout. All federal funding provided in this program must be expended or returned within eight years.

The new program offers a modern solution to the challenges of post-disaster recovery. By moving beyond the slow and reactive traditional PA program, it leverages States, Tribes, and Territories' autonomy, parametric funding, and transparent auditing to create a faster, more effective, and more accountable system for all Americans affected by disaster.

Reform the National Flood Insurance Program for Financial Stability and Risk Resilience

The Council recommends a comprehensive reform plan centered on a strategic shift toward a primary role for the private market, with the goal of fostering a more resilient and financially stable flood risk management system.



These changes are expected to accelerate disaster recovery, reduce the federal government's financial burden, send clear financial signals, and provide predictable financial outcomes for homeowners, ultimately leading to a more prepared nation.

Maximize Every Dollar Spent by Reducing Administrative Costs

To put Americans first, it is vital to maximize the efficiency of federal and SLTT dollars spent in emergency management.

Increased percentage of each federal dollar directly impacting affected Americans achieved through implemented efficiencies

Streamlined direct federal assistance programs

Reduced need for federal employees to deploy and/or manage direct programs

Decreased administrative costs for FSLTT

Highlighted reforms will reduce administrative and overhead costs, which preserves more of each federal or SLTT dollar to be spent on emergency management. Federal assistance reforms will create significant efficiencies that will generate upfront savings and increase the impact of each dollar distributed by accelerating the payments to enable faster recoveries.

Revitalize A Unified National Network for Partnership

The new framework would formalize and streamline coordination between government agencies, critical private-sector partners, and nonprofit organizations.

Whole Community Approach

Disasters demand a unified national effort that leverages the strengths of all sectors

Public-Private Coordination

Formalize and streamline coordination between government agencies, critical private-sector partners, and nonprofit organizations.

Shared Information

Develop and implement modern technology and communication protocols that ensure shared data and situational awareness among all partners

The transformed agency would address the existing gap in the emergency management landscape by returning to a network that enables government, private industry, faith-based, and non-profit partners to build toward a shared capability and integrated resources.

A Transformed Agency

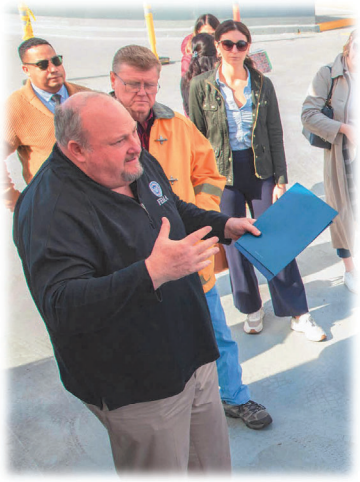
To address these shortcomings and national challenges in emergency management, transform FEMA into a new lean agency.

Review of Requirements
Conduct a strategic review to determine appropriate staffing levels against mission requirements.

Phased Approach
This transformation should be conducted over a 2-3 year phased approach.

Empower States
States will assume a greater role in managing disasters from preparedness to recovery, utilizing direct federal funding mechanisms.

Shift Training
While the future agency must establish and maintain national standards for disaster response, the direct execution of training should be shifted to the regional and state level.



The transformation is an imperative step toward restoring the agency's effectiveness, accountability, and public trust. By implementing a bold restructuring plan—centered on reviewing mission requirements, streamlining operations, eliminating redundancies, and empowering state partners—the federal government can ensure a more immediate, effective, and efficient response to disasters.

Implementation Requirements by Recommendation

While Executive Orders may be used to make some of the proposed changes, the Council advocates for legislative action to ensure a systemic and sustained transformation of the current approach to disaster management.

Recommendation	Minimum Action Required to Implement			
	Policy	Legislation	Regulation	Executive Order
#1 Equip SLTT to Lead	✓			
#2 Enhance Critical Programs	✓		✓	
#3 Realign Criteria for Assistance			✓	
#4 Replace HMGP		✓		
#5 Streamline IA		✓		
#6 Reform PA		✓		
#7 Reform NFIP		✓		
#8 Reduce Admin Costs				✓
#9 Network for Partnership	✓			
#10 Transform FEMA		✓		✓

It is important to note that all recommendations requiring legislative action will also need to be accompanied by regulations, but since they cannot be accomplished through regulation alone that action is not checked.

A more resilient AMERICA

These recommendations will lead to a more resilient *AMERICA*:

- ***A**ccelerate* disaster response and recovery
- ***M**odernize* systems and technology for greater efficiency
- ***E**mpower* local and state governments with better resources and tools
- ***R**educe* administrative costs and federal burden
- ***I**mprove* coordination across government, private sector, and nonprofits
- ***C**ultivate* public trust through transparency and accountability
- ***A**mplify* resilience for rural communities and critical infrastructure

These reforms aim to create a more resilient and prepared nation by ensuring that disaster response and recovery efforts are efficient, cost-effective, and locally executed. Such reforms also ensure that federal support will be available when significant events occur that overwhelm local systems.

Agenda:

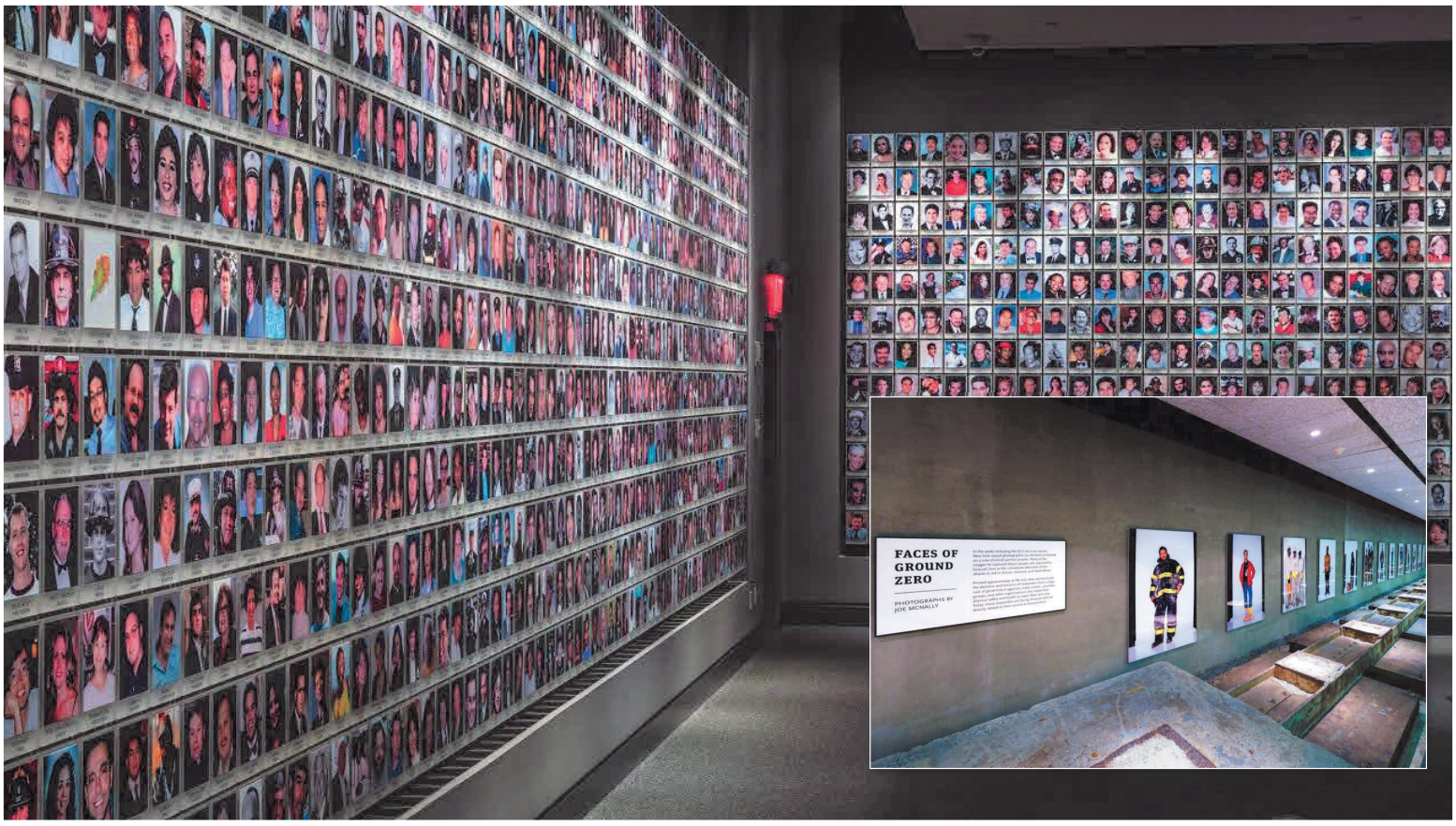
- Memorial Video Presentation
- September 11, 2001, Terrorist Attacks - looking back, looking forward
  - What changes did 9/11 produce?
  - Where do we stand now?
  - Where do we go from here?
- Homeland Security Discussion

Photo: Jin Lee

https://youtu.be/k2xy0ac-PGc?si=yHbXbECgrlQnxECf

25 years ago. Seems like yesterday.

Losses too great to bear.



Losses too great to bear

Victims: 2,977 people perished in New York City, at the Pentagon, and in Pennsylvania. This included civilians, passengers on the four hijacked flights, and military personnel.

First Responders: 441 first responders, including 343 firefighters and 72 law enforcement officers, were killed.

U.S. Service Members: Over 7,000 U.S. service members have died in direct combat and operations related to the post-9/11 wars, including more than 55 military personnel killed directly during the Pentagon attacks.

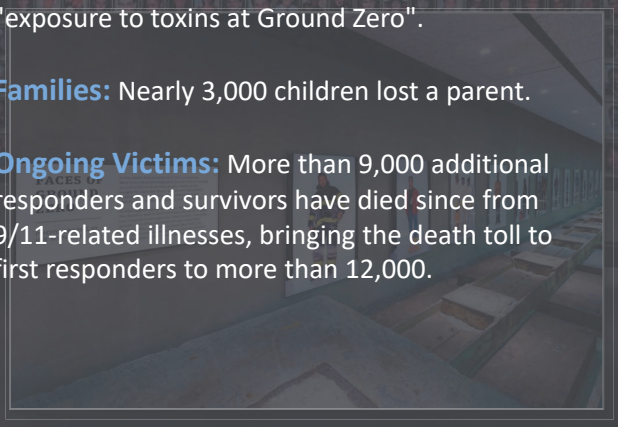
- An estimated 30,000 veterans and services members of post-9/11 conflicts have died by suicide.
- More than 8,000 U.S. contractors died in these theaters of operation.

Foreign Nationals: Foreign nationals from 61 countries perished in the 9/11 attacks.

Community Members: As of 2013, medical authorities concluded that 1,140 people from Lower Manhattan at the time of the attacks have been diagnosed with cancer as a result of "exposure to toxins at Ground Zero".

Families: Nearly 3,000 children lost a parent.

Ongoing Victims: More than 9,000 additional responders and survivors have died since from 9/11-related illnesses, bringing the death toll to first responders to more than 12,000.



Key changes that 9/11 produced.

Key changes that 9/11 produced

Major Legislation

- USA PATRIOT Act: Public Law 107-56, signed on October 26, 2001, expanding U.S. law-enforcement surveillance and counterterrorism powers after 9/11.
- Department of Homeland Security / Homeland Security Act (2002)
- Aviation and Transportation Security Act (2001)
- Intelligence Reform and Terrorism Prevention Act (2004)
- REAL ID Act (2005)
- Military Commissions Act (2006)
- Implementing Recommendations of the 9/11 Commission Act (2007)
- FISA Amendments Act (2008)

Aviation & Border Security

- No-Fly List & Terrorist Screening Database
- TSA Pre-Check (launched 2011)
- Secure Flight Program
- 100% Checked Baggage Screening

Emergency Management & Public Awareness

- Homeland Security Grant Programs (HSGP)
- National Incident Management System (NIMS) & Incident Command System
- "If You See Something, Say Something" Campaign
- FEMA Reforms / Post-Katrina Emergency Management Reform Act (2006)

Financial & Anti-Money Laundering

- Strengthened Bank Secrecy Act / Anti-Money Laundering Regime

Fusion Centers & Information Sharing

- National Fusion Center Network
- Homeland Security Information Network (HSIN)
- Terrorism Liaison Officer (TLO) Program

Immigration & Identity

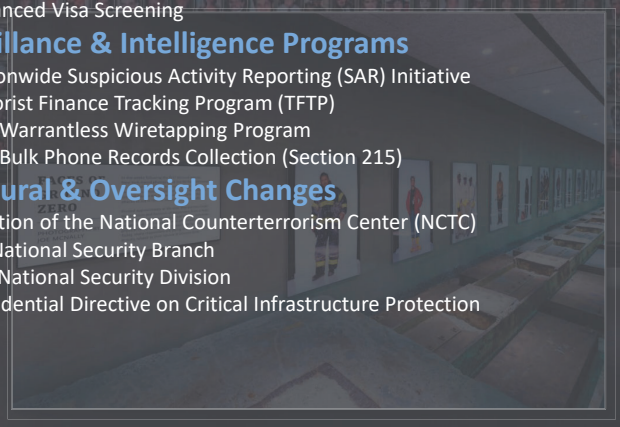
- Immigration Enforcement Expansion
- US-VISIT Program
- Enhanced Visa Screening

Surveillance & Intelligence Programs

- Nationwide Suspicious Activity Reporting (SAR) Initiative
- Terrorist Finance Tracking Program (TFTP)
- NSA Warrantless Wiretapping Program
- NSA Bulk Phone Records Collection (Section 215)

Structural & Oversight Changes

- Creation of the National Counterterrorism Center (NCTC)
- FBI National Security Branch
- DOJ National Security Division
- Presidential Directive on Critical Infrastructure Protection



Where do we stand?

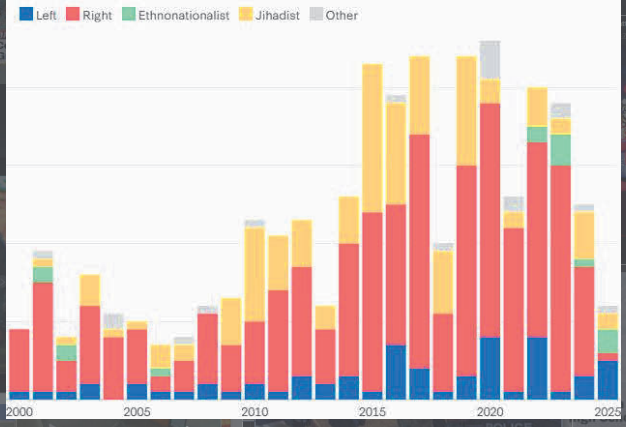
https://www.newamerica.org/

Where do we stand?

Where do we stand?

Ideological Trends in U.S. Terrorism

Terrorist Attacks and Plots in the United States by Perpetrator Orientation, 2000-2025*



Source: CSIS – Center for Strategic & International Studies

Anti-Government/Anti-Authority
- Anarchism
- Sovereign Citizens
- Militias/Sovereign Militias

Identity-Based & Misogynist Extremism
- Incels

Far-Left & Revolutionary Extremism
- Militant Anarchism/Anti-Capitalism
- Violent Sectarianism
- Revolutionary Communism

Racially and Ethnically Motivated Violent Extremism
- White Supremacism
- Neo-Nazism
- Black/Brown Separatism

Religious/Sectarian Violent Extremism
- Islamist Violent Extremism
- Militant Religious Fundamentalism

Single-Issue
- Anti-Abortion Extremism
- Eco-Terrorism
- Animal Rights Extremism

Mixed
- Conspiracy Extremism
- Nihilism

Where do we stand?

Ideological Inheritance

- The 9/11 attacks demonstrated to jihadist groups worldwide that spectacular violence against the U.S. was achievable. Al-Qaeda and later ISIS used this as a recruiting and propaganda tool. Some subsequent attackers, like the 2009 Fort Hood shooter and the 2015 San Bernardino attackers, explicitly cited jihadist ideology inspired by al-Qaeda or ISIS.

Tactical Diffusion

- Al-Qaeda and ISIS, diminished in external plotting and operational capabilities, are actively promoting "lone wolf" low-tech tactics (i.e., small arms assaults, crude bombs, vehicle ramming, knife attacks, arson, etc.) in response to their inability to execute another complex 9/11-scale attack. Publications like Inspire magazine provide guidance and has been attributed to numerous attacks.

The Security Paradox

- 9/11 led to massive hardening of "hard targets" (airports, federal buildings, landmark sites). This displacement effect pushed would-be attackers toward softer, harder to protect, targets, such as concerts, schools, houses of worship, retail stores, etc.

Important Distinction and Reality Check

- Domestic Violent Extremism (DVE) has emerged with several ideological drivers.
- Jihadist-inspired attacks comprise a minority of US-based post-9/11 mass violence.
- Many grievance-based mass shootings and active assailant attacks have been driven by mental health and social factors largely unrelated to 9/11.
- The full range of violent extremists learn from and adopt the tactics of other violent extremists, at times mimicking the TTPs of like-minded attackers.
- More routine active shooter response focus risks lowering the bar on more advanced terrorism response capabilities.

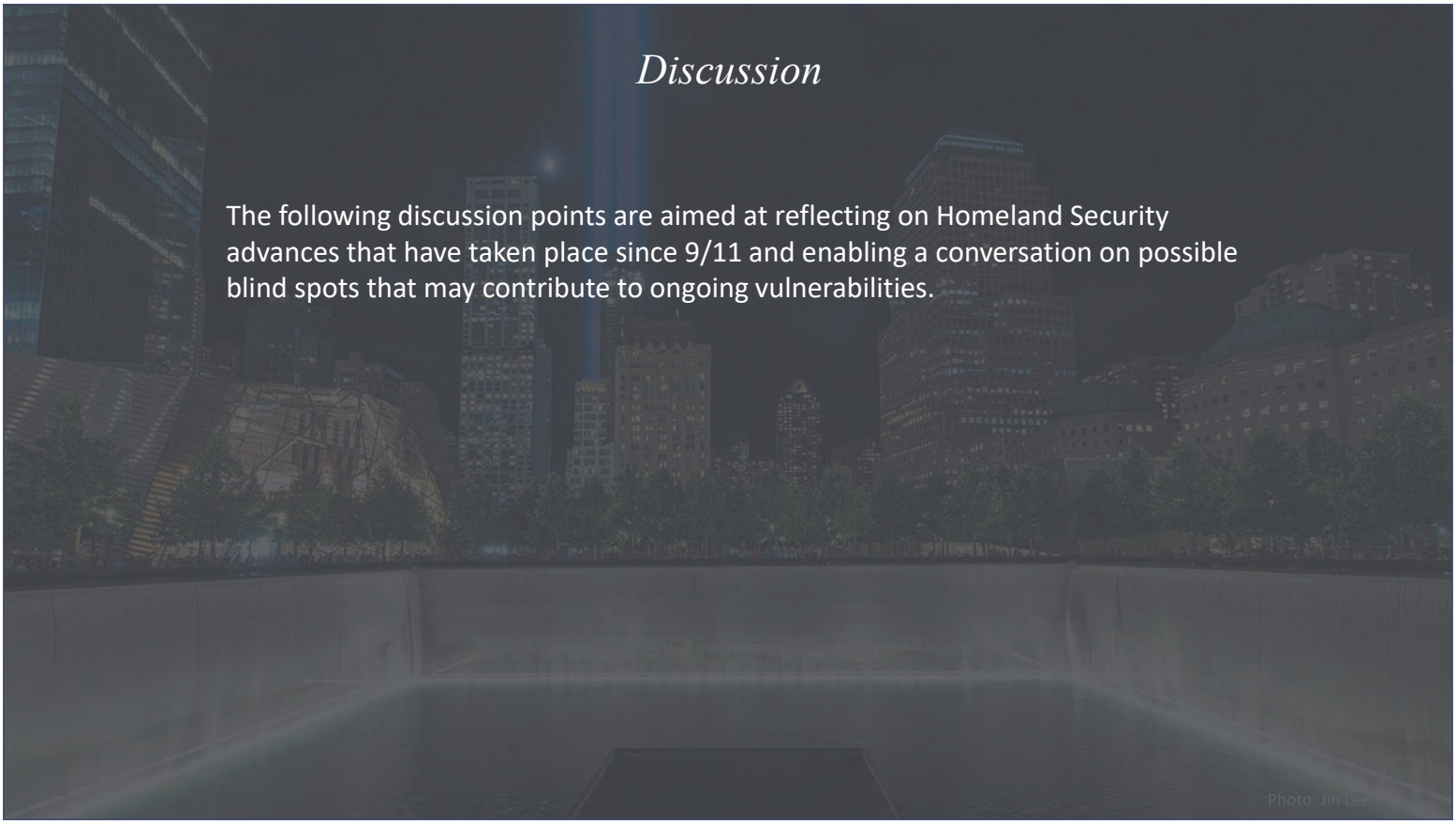
9/11 Homeland Security Advances

- The post 9/11 Homeland Security enterprise is positioned to address the broader array of threats, but success is a constantly moving target.

September 11, 2001 Terrorist Attacks & **Lessons Learned Over 25 Years**

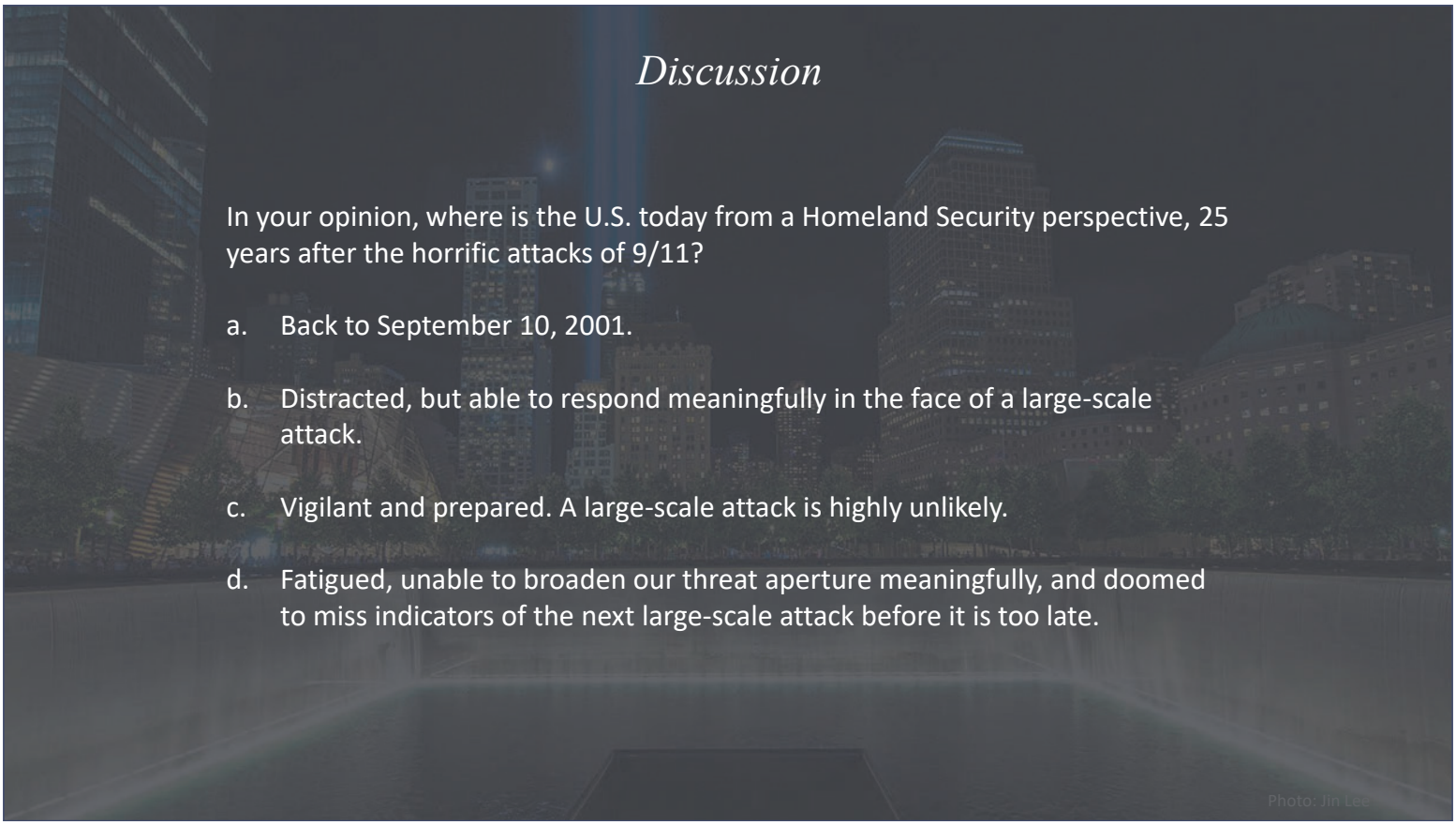
Interactive Discussion

Photo: Jin Lee



Discussion

The following discussion points are aimed at reflecting on Homeland Security advances that have taken place since 9/11 and enabling a conversation on possible blind spots that may contribute to ongoing vulnerabilities.



Discussion

In your opinion, where is the U.S. today from a Homeland Security perspective, 25 years after the horrific attacks of 9/11?

a. Back to September 10, 2001.

b. Distracted, but able to respond meaningfully in the face of a large-scale attack.

c. Vigilant and prepared. A large-scale attack is highly unlikely.

d. Fatigued, unable to broaden our threat aperture meaningfully, and doomed to miss indicators of the next large-scale attack before it is too late.

Discussion

Which of the listed post-9/11 homeland security initiatives continues to be critical in preventing acts of terrorism?

a. Establishment of fusion centers for real-time, multi-jurisdictional intelligence sharing.

b. Creation of the Department of Homeland Security (DHS) and unified federal coordination.

c. Development of the National Suspicious Activity Reporting (SAR) Initiative.

d. Implementation of the "If You See Something, Say Something" public awareness framework.

Photo: Jin Lee

Discussion

Which of the listed cross-sector partnerships do you consider to be of the highest importance in building national resilience against the largest threats?

a. Federal–state–local–tribal–territorial (FSLTT) coordination through regional planning structures.

b. Public-private partnerships for critical infrastructure protection and information sharing (ISACs).

c. Military–civilian coordination mechanisms (Defense Support to Civil Authorities — DSCA).

d. International law enforcement and intelligence partnerships (Five Eyes, Interpol, bilateral MOUs).

Photo: Jin Lee

Discussion

Which active threat/mass casualty response capability has most significantly improved since September 11, 2001 in your region?

a. Integrated law enforcement–fire–EMS unified command for complex incidents, such as Unified Response to Violent Incidents (URVI).

b. Active shooter / active threat response protocols (including ALERRT, STOP THE BLEED, etc.).

c. Enhanced training and equipment for specialized response teams (SWAT, HazMat, JHAT, etc.).

d. Mass casualty incident (MCI) triage systems and pre-hospital trauma care advances.

e. Tactical Emergency Casualty Care (TECC) integration across law enforcement.

Photo: Jin Lee

Discussion

If another 9/11-scale attack occurs, which of the listed factors will most likely have contributed?

a. A patient adversary that outlasts/outsmarts our national vigilance and detection capabilities.

b. A return to silos, leading to a lack of information-sharing across federal, state, and local agencies.

c. A lack of imagination enabling a major attack employing novel tactics.

d. Diminished counterterrorism focus or underestimating the evolving capabilities or foreign terrorist organizations.

Photo: Jin Lee

Discussion

Which technology or analytical capability advance do you see as the most transformative on public safety operations in the post-9/11 era?

a. Social media monitoring and open-source intelligence (OSINT) for situational awareness.

b. AI and data analytics for threat detection, predictive policing, and resource deployment.

c. Geospatial intelligence tools and GIS integration in emergency operations centers.

d. Unmanned aerial systems (UAS/drones) for surveillance, search and rescue, and damage assessment.

e. Biometrics and identity verification systems at ports of entry and in field operations.

Photo: Jin Lee

Discussion

What was the most significant Homeland Security failure in the US in the aftermath of 9/11, in your opinion? How do we avoid a similar failure going forward?

a. Boston Marathon Bombing

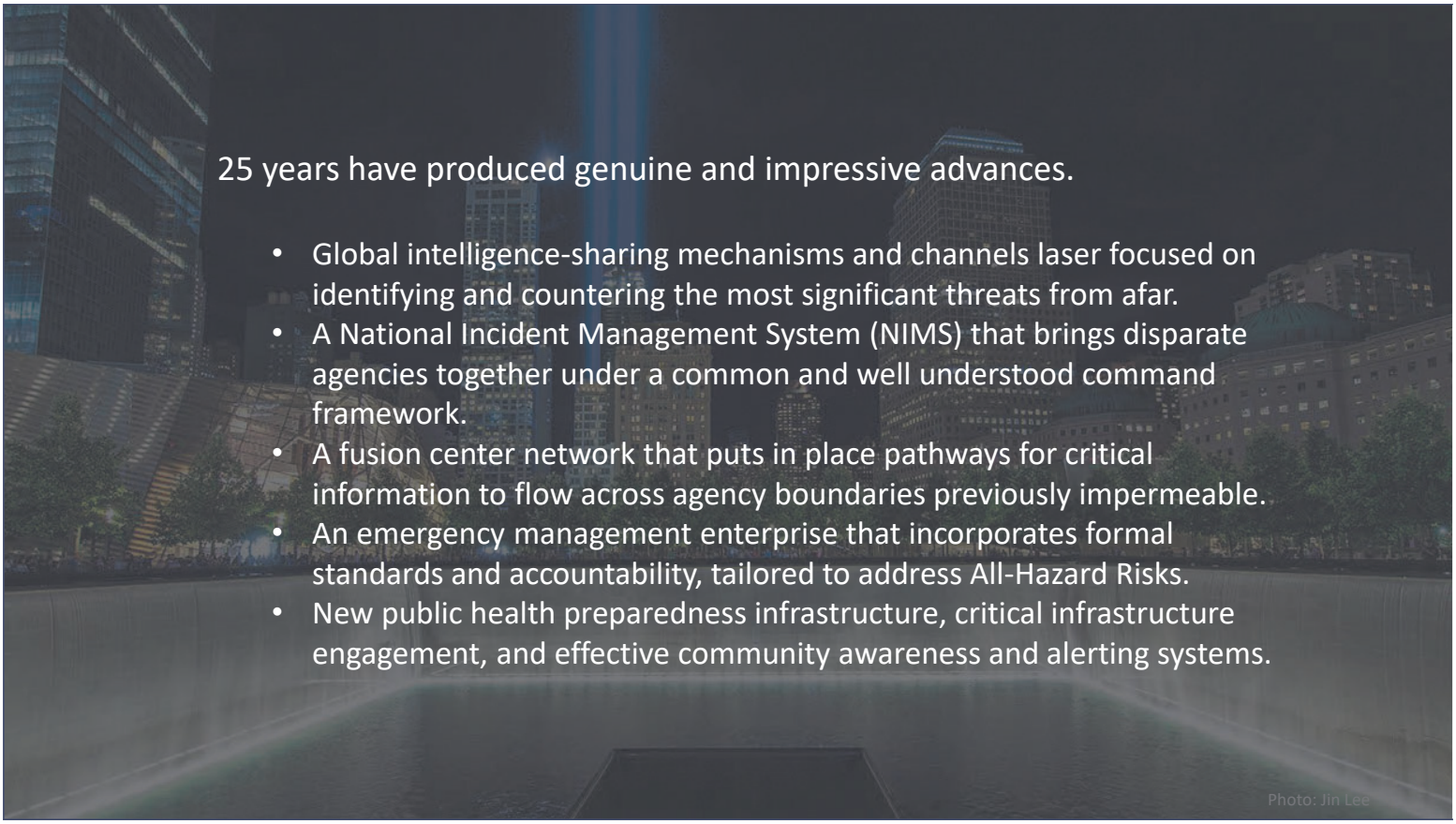
b. Las Vegas Route 91 Mass Murder

c. Pulse Nightclub

d. San Bernardino Terrorist Attack

e. Fort Hood

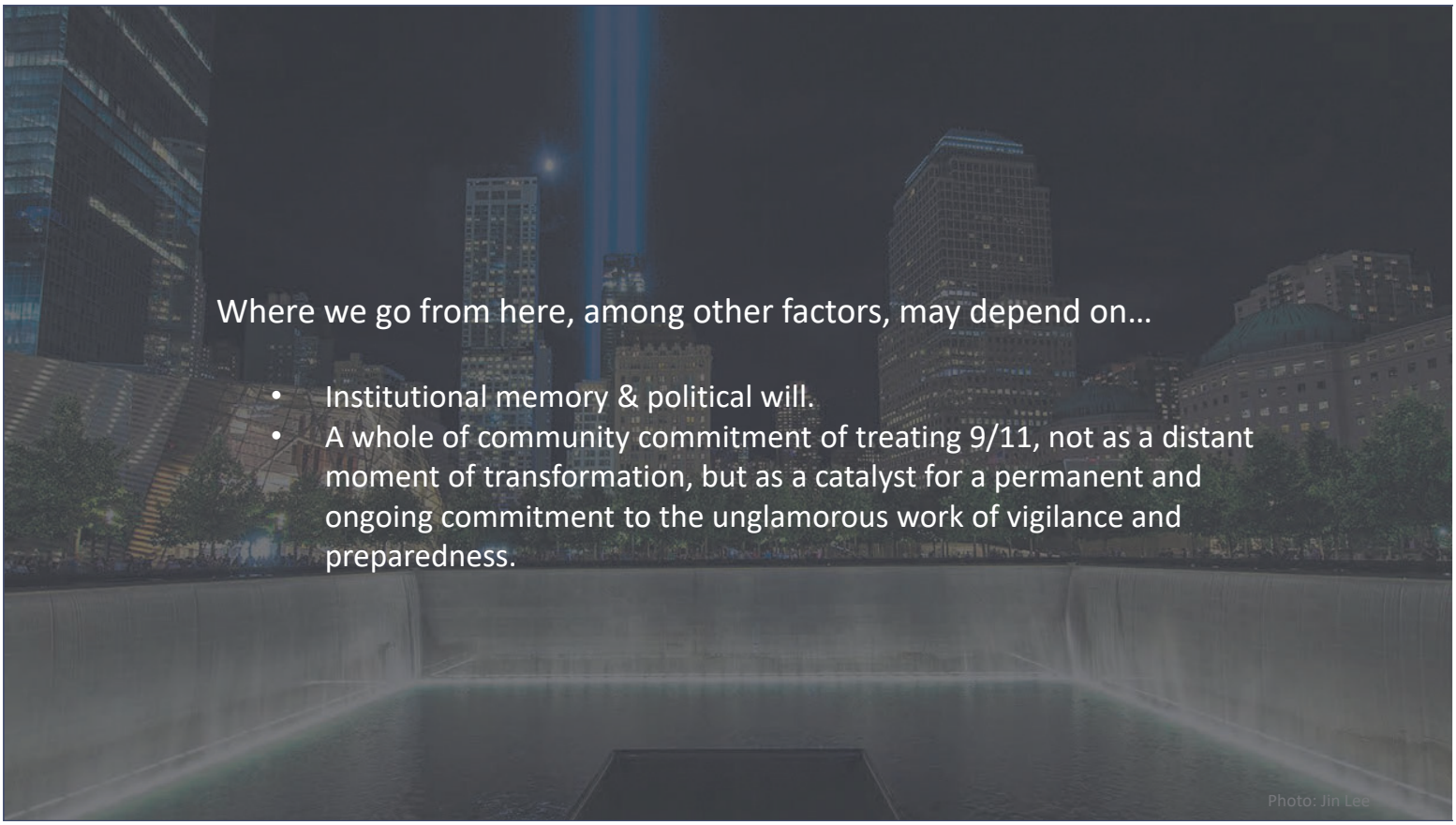
Photo: Jin Lee



25 years have produced genuine and impressive advances.

- Global intelligence-sharing mechanisms and channels laser focused on identifying and countering the most significant threats from afar.
- A National Incident Management System (NIMS) that brings disparate agencies together under a common and well understood command framework.
- A fusion center network that puts in place pathways for critical information to flow across agency boundaries previously impermeable.
- An emergency management enterprise that incorporates formal standards and accountability, tailored to address All-Hazard Risks.
- New public health preparedness infrastructure, critical infrastructure engagement, and effective community awareness and alerting systems.

Photo: Jin Lee



Where we go from here, among other factors, may depend on…

- Institutional memory & political will.
- A whole of community commitment of treating 9/11, not as a distant moment of transformation, but as a catalyst for a permanent and ongoing commitment to the unglamorous work of vigilance and preparedness.

Photo: Jin Lee

September 11, 2001
Terrorist Attacks &
Lessons Learned Over 25 Years

Memorial & Homeland Security Discussion

Photo: Jin Lee

Security Resilence Considerations for the National Homeland Security Consortium

John M. Gilligan, President and CEO

Rich Neely, Executive VP and GM of Operations, Intelligence, and Services (MS-ISAC)

Center for Internet Security

June 23, 2026

Topics

- Who is the Center for Internet Security
- Growing Security Threats for SLTT Organizations
- Changing Cyber Defense Environment
- Multi-State Information Sharing and Analysis Center
- Elections Infrastructure Information Sharing and Analysis Center

Who Is the Center for Internet Security?

Independent Nonprofit Working to Secure Our Connected World

- **Mission-Driven and Independent, Not Profit-Driven**
  - As a nonprofit, CIS is uniquely driven to serve the U.S. SLTT community
- **Global Standards Leader**
  - CIS has been a leading provider of cyber best practices for 25+ years
  - CIS Critical Security Controls have been identified as a minimum cyber standard in six U.S. states and downloaded by over 600,000 organizations worldwide
- **Providing a Collaborative Cyber Defense Ecosystem**
  - Our goal is to strengthen the SLTT community's collective defense, resilience through shared intelligence, best practices, threat defeating products, and peer collaboration

Examples of CIS's Thought Leadership

Proven Cyber Defensive Solutions

- **CIS Configuration Benchmarks**
  - Over 100 vendor products
  - Hardened Images of benchmarks on all major cloud offerings
- **CIS Security Controls**
  - 18 Controls with 54 Safeguards
  - Essential Cyber Hygiene (Level 1 Safeguards)
- **" CIS Community Defense Model, Version 2.0"**
- **"A Guide to Defining Reasonable Cybersecurity"**
- **"Secure by Design: A Guide to Assessing Software Security Practices"**
  - Prioritized and measurable software development practices

Secure Cyber Cities

CIS Helping Cities Strengthen Cyber Resilience

- **One-of-a-kind Program**
  - Delivers tailored cybersecurity tools, audits, and intrusion detection for U.S. cities
  - Builds community-wide cyber awareness through training and education
- **Stamford, CT: Pilot Success Story**
  - 18-month pilot demonstrating whole-city cybersecurity collaboration
  - Achievements included resident training, partnerships to security cyber improvement grants, and enhanced feedback systems
  - Stamford's collaboration now serves as a model for cities nationwide working to strengthen whole-of-city cyber resilience
- **Annapolis MD, Lansing MI, Redland CA, and other cities being evaluated for Secure Cyber City initiatives**

Topics

- Who is the Center for Internet Security
- Growing Security Threats for SLTT Organizations
- Changing Cyber Defense Environment
- Multi-State Information Sharing and Analysis Center
- Elections Infrastructure Information Sharing and Analysis Center

The Cost of Cyber Crime

Cybersecurity Is Homeland Security — **SLTTs Are Our Frontline Defense**

Cyber related crime is the most pervasive and expensive threat challenging the economic and physical security of the U.S.

$100B
Domestic Counterterrorism*

$150B
Natural Disaster Response†

$639B
Cybercrime‡

*Homeland Security Today: The Costs of Targeted Violence and the Value of Investing in Prevention
†Climate.gov: 2024: An active year of U.S. billion-dollar weather and climate disasters
‡Statista.com: Estimated annual cost of cybercrime in the United States from 2017 to 2028

AI: Escalating Threats — CIS Leading the Defense

- **AI Is Accelerating Cyber Risks**
  - GenAI amplifies phishing, exploit automation, and supply-chain model poisoning
  - Prompt hijacking/jailbreaks bypass safeguards to extract sensitive data
  - Federal shift toward cyber offense widens the protection gap for SLTTs
  - Agent-based AI introduces a new level of threat
  - New Mythos and GPT 5.5-Cyber models accelerate discovery of vulnerabilities

- **CIS: National AI Leadership for SLTT Defense**
  - MS-ISAC AI Playbooks: Readiness, Governance, Risk Review, Procurement
  - Responsible AI guidance, transparency templates and secure prompt training
  - AI application assessments with targeted penetration testing
  - In discussions with OpenAI to assist states in leveraging GPT 5.5-Cyber
  - Embedding AI in CIS's defenses to keep pace with AI-enabled threats

Countering Multi-Dimensional Threats

- **Supporting SLTT organizations to enhance ability to prepare for, detect, and respond to emerging multidimensional threats**
  - Working closely with law enforcement, homeland security, emergency management, and cyber-security officials
  - Providing rapid detection and warning of cyber, internet-enabled physical, and disruptive threats (information operations, swatting, bomb-threats, etc...)
- **Emphasis on special events such as FIFA World Cup and elections**
- **Recent products address countering cyber and physical threats**
  - Unmanned Aviation Vehicles (drones)
  - Threats to government officials
  - Synthetic media content (deep fakes)
  - Cyber-enable intelligence gathering targeting law enforcement (UTS)

Topics

- Who is the Center for Internet Security
- Growing Security Threats for SLTT Organizations
- Changing Cyber Defense Environment
- Multi-State Information Sharing and Analysis Center
- Elections Infrastructure Information Sharing and Analysis Center

Contemporary Environment

Threats and challenges facing the public sector

- **SLTT Cyber Risk Is Increasing**
  - Advanced nation-state threats, increasingly leveraging AI, targeting SLTTs daily
  - Cyber, physical attacks growing in scale and sophistication
- **Federal Support Declining**
  - SLCGP reduced by 67% from FY24 to FY25 ($280M to $91.7M) and has now ended
  - Major cuts to CISA-funded programs and personnel, reducing CISA support and program capacity
  - 2025 Executive Order shifts cybersecurity responsibility to state/local levels
- **Result**
  - SLTTs face greater burden with fewer resources
  - Under-resourced public-sector and critical infrastructure entities most at risk

State, local, tribal, and territorial alignment is vital now more than ever

Topics

- Who is the Center for Internet Security
- Growing Security Threats for SLTT Organizations
- Cyber Defense Environment
- Multi-State Information Sharing and Analysis Center
- Elections Infrastructure Information Sharing and Analysis Center

The MS-ISAC: Helping Defend the Nation

By the Numbers

MS-ISAC support to SLTT organizations in 2025	
Detected Cyber Incidents†	86,638
Blocked attempts to connect to known malicious sites online	9.1B
Threat indicators shared with members	> 123k
Intelligence reports share with members	92

†Total number of Albert Network Monitoring, CIS Managed Detection and Response (MDR), and Managed Security Services (MSS) cases detected and escalated

"The [MS-ISAC] has helped raise the bar and establish a stronger operational standard for integrated threat monitoring and information sharing across cyber and physical security domains."

Mike Sena | Northern California Regional Intelligence Center

MS-ISAC: Supporting Whole-of-State Efforts

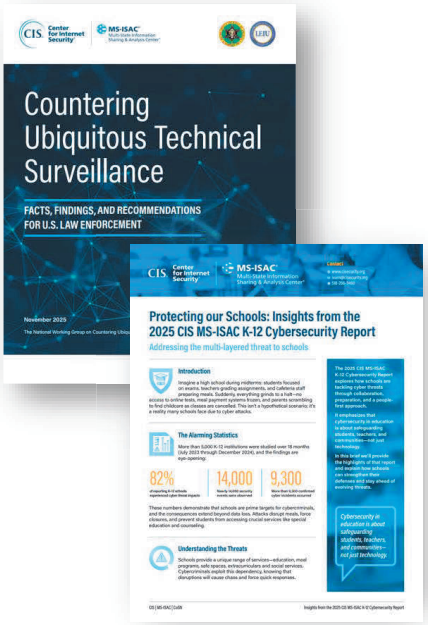
Establishing a Unified Approach to Security

A **whole-of-state approach** extends beyond executive-level agencies to engage stakeholders **across sectors and levels of government** as well as private industry in a **coordinated, collaborative risk management process.**

MS-ISAC Provides:

- Support for state leaders
- Support to states in **building relationships with local organizations**
- A **statewide dashboard** showing critical information across all member organizations in the state
- Facilitation of **data sharing** and **improved coordination** between state and local entities
- Support to align statewide member participation and training to meet state goals

MS-ISAC: Sector-Relevant Collaboration & Insights



Uniquely Unifying SLTT Sectors with Shared Threat Intelligence and Defense

- Nationwide, sector-specific intelligence from SOC telemetry, incident response cases, cybersecurity assessment reporting (e.g., K-12 Report)
- Peer collaboration that improves outcomes
- High-impact cyber defense products, including web security (protective DNS)
- Executive-level threat and informational products
- Centralized engagement in form of MS-ISAC leads to faster recovery, less disruption within and across sectors

MS-ISAC: Active Support to Law Enforcement

Actionable Multidimensional Threat Intelligence

The Washington Times
America's Newspaper

This national program can help stop police network hackers

Restore funding for the MS-ISAC

By Craig Apple - Tuesday, September 23, 2025

OPINION:

America's law enforcement agencies and departments are under siege, not by armed assailants but by cybercriminals. These threat actors are no longer just stealing data but actively disrupting the systems that keep communities safe. Through tactics such as ransomware attacks that cripple jail management systems or hackers infiltrating sensitive police networks, these digital assaults are derailing law enforcement operations, endangering officers and compromising critical investigations.

The good news is that there is a solution. Every day, hundreds of sheriff's offices like mine rely on a national program called the Multi-State Information Sharing and Analysis Center to protect our communities' digital backbones. The MS-ISAC provides critical resources to protect dispatch systems, jail networks, court records and 911 emergency communications.

Since January 2024, MS-ISAC services have prevented 57 cybersecurity incidents specifically targeting more than a dozen law enforcement organizations and blocked more than 40 million threat events across nearly 60 law enforcement organizations. Each of these incidents had the potential to cause significant disruption to communities across the country.

"Every day, hundreds of sheriff's offices like mine rely on a national program called the Multi-State Information Sharing and Analysis Center to protect our communities' digital backbones. The MS-ISAC provides critical resources to protect dispatch systems, jail networks, court records and 911 emergency communications."

Sheriff Craig Apple | **Albany County, NY**
2024 National Sheriff of the Year,
National Sheriff's Association

MS-ISAC: Nationwide Collective Defense

A Comprehensive Cyber Defense Ecosystem for the Public Sector

Every public sector entity in your state is a target.
The MS-ISAC helps make them a team.

- **The MS-ISAC provides:**
  - Unified, coordinated defense
  - Shared threat intelligence
  - Proven best practices and peer collaboration
  - Tools/services custom-built for public sector
  - Statewide risk reduction

As of May '26

23	42%	>22.8k
participating states/ territories	of the U.S. population protected	eligible members covered

Why the MS-ISAC Matters

MS-ISAC's Essential Value Proposition

State and Local Leaders Are Asking:

- Can each state protect its own agencies? **Maybe?**
- Can it share threat intelligence with all towns and counties? **Maybe?**
- Can it communicate threats nationwide? **No!**

MS-ISAC: The *Only* Nationwide Community Defense Network

- Centralized, **bi-directional info sharing** strengthens national security
- **Real-time collaboration** turns isolated efforts into a coordinated system
- ISACs enable **cross-sector responses** to cyber/physical threats
- DHS CISA does not perform this function
- The states do not perform this function
- Without it, the nation is "flying blind" and is less secure

MS-ISAC: Driving Public, Private Collaboration

Bringing Leading Tech Partner Solutions to States and Locals

- **Longstanding partnerships with:**
  - Google, AWS, Microsoft
  - CrowdStrike
  - Akamai
- **SLTT membership organization partnerships:**
  - **Big 7 Associations:** NGA, NCSL, NLC, USCM, NACo, CSG, ICMA
  - **Other SLTT member organizations:** Major County Sheriffs of America (MCSA), Consortium for School Networking (CoSN), etc.

*"The idea that every public sector organization should build out their own security team and go out and hire their own CIO and CISO…if you got deep pockets and a high tax base, and you can afford it, that's great, but the vast majority can't. So what are they supposed to do? They should be partnering with organizations. And **this is where the value of the MS-ISAC jumps out to me.**"*

MK Palmore, Google Cloud

*"The Center for Internet Security (CIS) has been **an invaluable partner**, largely because we have a shared vision…[to] increase the security posture of state, local government, and academic institutions in need."*

Maria Thompson, AWS

MS-ISAC: A Strategic Partner for States

Community Defense. Actionable Threat Intel. Unified Security.

An unmatched community defense **network of resources and experts** devoted to thwarting public sector cyber threats.

The nation's trusted source for actionable **multidimensional threat intelligence** — powered by the largest public-sector threat database.

We're not a vendor. We're a **strategic partner** driving unified security and risk reduction across state and local governments.

Topics

- Who is the Center for Internet Security
- Growing Security Threats for SLTT Organizations
- Changing Cyber Defense Environment
- Multi-State Information Sharing and Analysis Center
- Elections Infrastructure Information Sharing and Analysis Center

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

Strengthening the Cyber Posture and Resilience of Election Offices

Annual Election Threat Assessments

Strategic insight into physical, cyber, and foreign malign information threat trends likely to impact elections. These assessments enhance organizations' ability to make long-term resource decisions to enhance security.

Emerging Election Incident Alerts

Timely alerts about near-term, rapidly evolving physical, cyber, and foreign malign information threats to elections. These concise updates help organizations make rapid threat mitigation decisions.

ThreatWA™ Weekly Election Executive Update

Weekly analysis of election-related physical, cyber, and foreign malign information threats and trends. These reports enhance an organization's ability to make near- and medium-term decisions to protect their interests.

Virtual and In-Person Election Threat Briefings

Periodic virtual and in-person election briefings which will allow election officials to hear directly from and pose questions to analysts covering physical, cyber, and foreign malign information threats.

Critical Trend Reports

Periodic, in-depth analysis of specific physical, cyber, and foreign malign information threat trends and tactics that may impact elections. These reports provide organizations with insights they can use to strengthen their defenses against targeted threats.

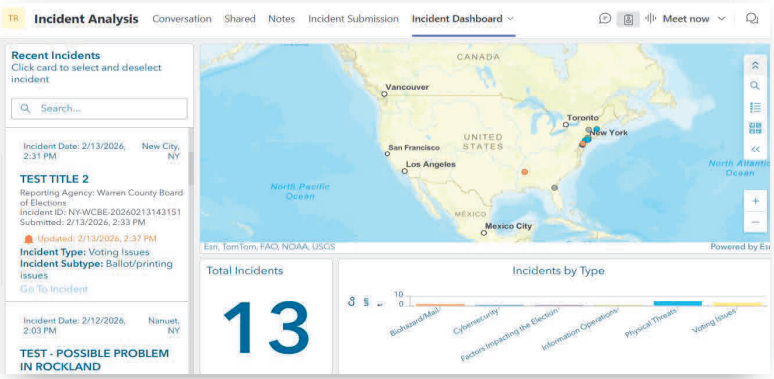
Security Devices and Tabletop Exercises

Security devices protect key election infrastructures. Exercises with election offices, law enforcement and emergency responders ensure proper preparation.

EI-ISAC Situational Awareness Room (SitRoom)

Sharing Threat Information in Near Real-time

- **Provides election officials, technology providers and associations a secure platform to share and receive cyber, physical, and foreign malign threats**
  - Open for statewide primaries/general election



Center for Internet Security

Questions/Discussion