State, Local, Tribal, and Territorial Government Coordinating Council

Sector-Specific Plan Annex to the NIPP 2013

2015

Homeland Security

Contents

COORDINATION LETTER FROM COUNCIL CHAIRS

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC, Council) is a national cross-sector council under the National Infrastructure Protection Plan 2013 (NIPP 2013) partnership structure. Since its designation in 2007 by the Federal Government, the Council has served as the organizational structure to voluntarily coordinate across jurisdictions and disciplines to provide senior-level strategic communications and coordination on State, local, tribal, and territorial (SLTT) agency security and resilience initiatives, activities, and best practices.

This 2015 SLTTGCC Annex to the NIPP 2013 describes SLTT critical infrastructure assets and risks, partnership activities for security and resilience, and Council goals and priorities to guide the community's critical infrastructure efforts over the next four years. The Council's goals and priorities closely align with the NIPP 2013, 2014 Joint National Priorities for Critical Infrastructure Security and Resilience, and Executive Order 13636: Improving Critical Infrastructure Cybersecurity. SLTT critical infrastructure programs are actively implementing a partnership approach to security and resilience; sharing information across the critical infrastructure community; and ensuring coordinated, comprehensive risk management.

Recent SLTTGCC accomplishments highlighting the successes of the partnership include:

- **Council meetings, calls, and Webinars** facilitate discussion among members, subject matter experts, and Alliance Networks on critical infrastructure issues and real-life applicability of solutions and programs, tailored to jurisdictions based on their needs, capabilities, and resources.
- **SLTTGCC working groups** maintain regular communication with Federal program offices to provide the SLTT perspective on Federal policy, programs, tools, and capabilities, including NIPP 2013 and Sector-Specific Plans development; the development and implementation of IP Gateway; and the enhancement of the Regional Resiliency Assessment Program.
- **Regional activities** have expanded the Council's network and ability to integrate SLTT security and resilience efforts nationally. Examples include developing a baseline of the composition, activities, and needs of SLTT critical infrastructure programs across the Nation and collaborating with the U.S. Department of Homeland Security Office of Infrastructure Protection on an initiative to build regional capacity of critical infrastructure programs and capabilities.
- **SLTTGCC collaboration with the other NIPP partnership councils** has increased, which has enabled the Council to expand its network, provide the SLTT perspective, and educate others on critical infrastructure issues.
- **The SLTTGCC hosts regular virtual engagements** to convene SLTT partners across the country via Webinar to learn more about and discuss critical infrastructure issues, such as Federal Emergency Management Agency grants, the Threat and Hazard Identification and Risk Assessment process, and the National Counterterrorism Center's State and local programs.

These achievements represent the effective collaboration of the Council with SLTT agencies, other national councils under the NIPP 2013 partnership structure, and the Federal Government. They clearly demonstrate the Council's progress and collaborative approach to developing, prioritizing, and implementing effective security programs and resilience strategies.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013 and Executive Order 13636, SLTTGCC partners look forward to continuing their efforts to enhance the security and resilience of the Nation's critical infrastructure assets.

Curtis A. Parsons Jr

Curtis Parsons
Chair, SLTTGCC
Homeland Security and Emergency Management Coordinator,
Lenawee County, Michigan

Caitlin A. Durkovich
Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security

Brian Wright
Vice Chair, SLTTGCC
Director, Critical Infrastructure Program,
State of New York

EXECUTIVE SUMMARY

State, local, tribal, and territorial (SLTT) governments execute the critical infrastructure mission as entities responsible for ensuring the security and resilience of their jurisdiction and/or as owners and operators of assets, systems, and networks. SLTT critical infrastructure programs are actively implementing a partnership approach to security and resilience; sharing information across the critical infrastructure community; and ensuring coordinated, comprehensive risk management. SLTT owners and operators provide for a wide range of services necessary for a safe and functioning society. A failure or disruption to SLTT critical infrastructure could result in significant harm or loss of life, major public health issues, long term economic loss, and/or cascading disruptions and escalating impacts to other critical infrastructure.

SLTT Assets and Risks

SLTT governments establish critical infrastructure programs to formalize their approach to achieving the security and resilience of infrastructure critical to their communities' sustainability. In addition, SLTT agencies own and/or operate assets in several critical infrastructure sectors: Communications, Dams, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Transportation Systems, and Water and Wastewater Systems. The human, physical, and cyber assets in these sectors provide for many essential services necessary for a secure society, including government operations, energy and water utilities, education systems, public health, and emergency response. Risks to the ability for SLTT governments, owners, and operators to provide these essential services include managing an all-hazards portfolio, operating in a resource-constrained environment, and needing to increase knowledge and awareness of critical infrastructure issues, tools, programs, and policies.

Partnering to Improve Security and Resilience

SLTT governments establish and participate in public-private partnerships to facilitate coordinated information sharing and enable planning and preparedness within and across jurisdictions. These partnerships serve as crucial coordination hubs, bringing together prevention, protection, mitigation, response, and recovery authorities, capacities, and resources among local jurisdictions, across sectors, and between regional entities. Operating as sector-specific or cross-sector, and under a variety of governance structures, partnerships strengthen the ability to prepare for, withstand, and recover from disruptions.

At the national level, the National Infrastructure Protection Plan 2013 (NIPP 2013) partnership structure enables SLTT personnel to participate actively in national critical infrastructure security and resilience efforts. Since 2007, the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC, Council) has served as the organizational structure to voluntarily coordinate across jurisdictions and disciplines to provide senior-level strategic communications and coordination on SLTT agency security and resilience initiatives, activities, and best practices. Membership diversity (e.g., between levels of government and among disciplines), regular management of security and resilience issues, and longevity through administrations positions the Council to influence and directly support the implementation of the Nation's critical infrastructure security and resilience mission.

Recent SLTTGCC accomplishments highlighting the successes of the partnership include:

- **Council meetings, calls, and Webinars** facilitate discussion among members, subject matter experts (SMEs), and Alliance Networks on critical infrastructure issues and real-life applicability of solutions and programs. This has led to replication of initiatives and programs across the country, scalable to each jurisdiction based on their needs, capabilities, and resources.
- **SLTTGCC working groups** maintain regular communication with Federal program offices to provide the SLTT perspective on Federal policy, programs, tools, and capabilities. The Council contributed to the drafting of documents, such as the NIPP 2013 and the Sector-Specific Plans (SSPs); the development and implementation of IP Gateway and its transition from the Automated Critical Asset Management System (ACAMS); the enhancement of the Regional Resiliency Assessment Program (RRAP) by linking physical and cyber components; and the sharing of best practices for pandemic influenza preparedness and response.
- **Regional activities** have expanded the Council's network and ability to integrate SLTT security and resilience efforts nationally. The Council's Regional Initiative (2011–2013) developed the first-ever baseline of the composition, activities, and needs of SLTT critical infrastructure programs across the Nation. Findings from the initiative guided Federal program enhancements, Council strategic planning and information-sharing activities, and phase 2 of the initiative (Regional Overview of Critical Infrastructure Programs 2015-2016) to document

changes over time and update SLTT and partnership needs to be filled by the Council and/or Federal programs. Starting in 2015, the Council has collaborated with the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) on an initiative to build regional capacity by encouraging local and regional collaboration and implementation of activities consistent with national goals.

- **SLTTGCC collaboration with the other NIPP partnership councils** has increased, which has enabled the Council to expand its network, provide the SLTT perspective, and educate others on critical infrastructure issues. Primary examples include working with the Regional Consortium Coordinating Council (RC3) to implement the Regional Overview project and developing the Joint Critical Infrastructure Partnership (JCIP) Webinar series.
- **The SLTTGCC hosts regular virtual engagements,** such as the Real-Time Forums, to convene SLTT partners across the country via Webinar to learn more about and discuss critical infrastructure issues. Topics discussed in 2014-2015 include Federal Emergency Management Agency (FEMA) grants, the Threat and Hazard Identification and Risk Assessment (THIRA) process, RRAP, the Resilience Implementation Process, and the National Counterterrorism Center's State and local programs.

2015 SLTTGCC Planning

As part of this 2015 SLTTGCC Annex, the SLTTGCC identified goals and priorities to guide the community's security and resilience efforts over the next four years. The five goals are:

- **Grow and Mature the Council**—Enable the Council to mature and become agile in order to meet its requirements under the NIPP 2013, accomplish goals and priorities, and effectively represent SLTT perspectives.
- **Inform the Changing Critical Infrastructure Landscape**—Identify and articulate changes in the SLTT critical infrastructure mission and educate others on operating within the changed landscape.
- **Engage SLTT Government Partners on Critical Infrastructure Issues**—Leverage the Council's working groups, initiatives, and products to educate colleagues in other jurisdictions on critical infrastructure issues.
- **Collaborate with the Critical Infrastructure Community**—Work with DHS, other DHS partnership councils (e.g., National Infrastructure Advisory Council, Sector Coordinating Councils (SCCs), and Government Coordinating Councils (GCCs)), the critical infrastructure sectors, and other partners on projects of common interest.
- **Contribute to National Critical Infrastructure Policies and Federal Programs, Tools, and Capabilities**—Leverage the Council's working groups to collaborate with DHS to ensure Federal critical infrastructure policies, plans, programs, tools, and capabilities meet SLTT government needs.

To achieve these goals, the Council developed 14 priorities to focus their efforts. The priorities include meeting the Council's requirements under NIPP 2013; serving as a change agent in the evolving critical infrastructure mission space; collaborating with primary stakeholders (e.g., SLTT partners, the critical infrastructure community, and DHS); and contributing the SLTT government perspective to Federal policies, plans, tools, programs, and capabilities. In addition, the Council identified 26 activities to conduct, as resources allow, to improve the security and resilience of the SLTT critical infrastructure community in the United States. The activities focus on ensuring the Council remains a robust organization that consistently provides value to the critical infrastructure community, leveraging a number of high-priority Federal critical infrastructure programs by SLTT agencies, and collaborating with specific organizations on issues of common interest.

As a result, progress toward sector goals, priorities, and activities contributes directly to national achievements under the NIPP 2013. Appendix B demonstrates the detailed alignment of the SLTTGCC SSP Annex to NIPP 2013 goals, the Joint National Priorities, and NIPP 2013 Calls to Action.

1. INTRODUCTION

This 2015 State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) Sector-Specific Plan (SSP) Annex to the National Infrastructure Protection Plan 2013 (NIPP 2013) is designed to guide voluntary, collaborative efforts to improve State, local, tribal, and territorial (SLTT) agencies' security and resilience over the next four years. It describes how the SLTT critical infrastructure community manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. As a supporting plan to the NIPP 2013 and the SSPs, this document tailors the strategic guidance and risk management framework in the NIPP 2013 to the unique operating conditions and risk landscape of the SLTT community.

Most importantly, this document sets the strategic direction for SLTT security and resilience efforts by identifying shared goals, priorities, and activities for partners. Developed by representatives of the SLTTGCC, this Annex identifies a collaborative approach to mitigate critical infrastructure risks and maximize limited resources.

This SLTTGCC SSP Annex answers NIPP 2013 Calls to Action #2 and #3, which focus on articulating shared priorities and activities that build sector, SLTT, and regional capacity and increase coordination with the emergency management community. As a national, voluntary partnership council under the NIPP 2013, the SLTTGCC provides the organizational structure to strategically coordinate with multiple stakeholders—including across jurisdictions and disciplines, with DHS, and with other NIPP 2013 partnership councils. Facilitating senior-level strategic communications and coordination on SLTT agency initiatives, activities, and best practices enables the Council to take a central role in security and resilience; educate others on implementation of the NIPP 2013; and meaningfully contribute to the improvement of Federal critical infrastructure programs, tools, and capabilities utilized by SLTT agencies.

This SLTTGCC SSP Annex includes the following elements:

- **Chapter 2: Asset and Risk Profile**—Describes the major components of SLTT agencies and assets, risks facing SLTT governments and SLTT owners and operators, sector-specific risks that SLTT agencies can help plan for and mitigate, and key partnerships.
- **Chapter 3: Risk Management**—Describes SLTT risk management activities—identify assets, understand risks and interdependencies, and share information—how SLTT governments are addressing the most common significant topical risk areas, and the SLTT critical infrastructure risk management program activity outlook.
- **Chapter 4: Vision, Mission, Goals, and Priorities**—Presents the SLTTGCC's vision for security and resilience; mission to enact that vision; and updated goals and priorities to support NIPP 2013 goals, Calls to Action, and Joint National Priorities. Lists the specific activities the SLTTGCC plans to undertake to address the priorities, as well as the planned approach to measure the effectiveness of the activities.
- **Appendices**—Provide additional detail to support the major chapters of this Annex.

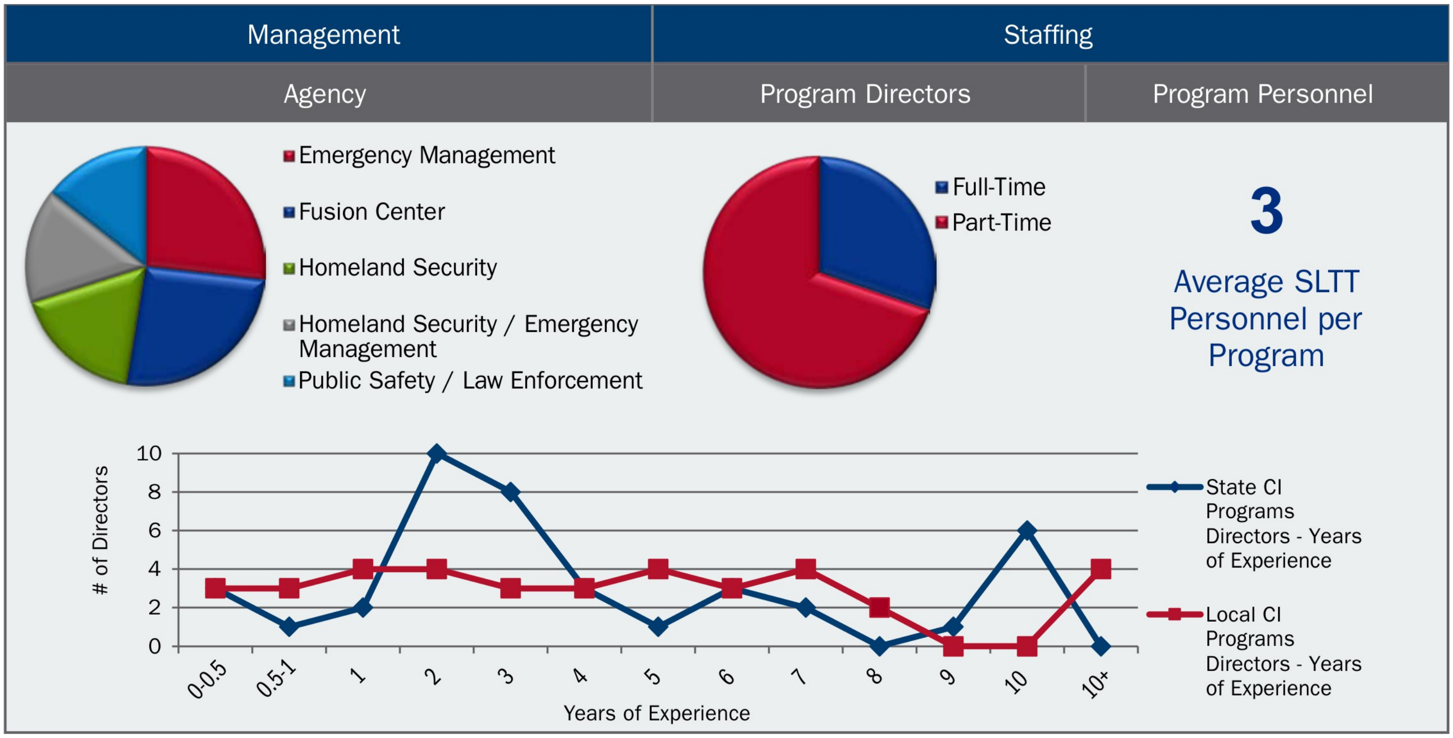
2. ASSET AND RISK PROFILE

SLTT governments contribute to the national critical infrastructure mission by ensuring the security and resilience of their jurisdiction, which may include maintaining critical assets, systems, and networks as owners and operators. The establishment of SLTT critical infrastructure programs enables a systematic risk-management approach to security and resilience in a given jurisdiction. To ensure a safe and functioning society, SLTT owners and operators manage a variety of human, physical, and cyber assets that provide for a wide range of essential services, including government operations, energy and water utilities, education systems, public health, and emergency response. In addition to managing their jurisdiction's asset portfolio, SLTT governments and owners and operators consider risks (including those related to dependencies and interdependencies) to their ability to provide essential services. Managing for all-hazards, operating in a resource-constrained environment, and needing to increase knowledge and awareness of critical infrastructure issues, tools, and programs may erode or threaten the ability for SLTT governments and owners and operators to maintain security and resilience across their entire asset portfolios.

2.1 Critical Infrastructure Programs

SLTT governments establish critical infrastructure programs to formalize their approach to enhance the security and resilience of infrastructure specifically critical to their communities. These programs vary considerably between jurisdictions, with no two jurisdictions exactly alike in assets, capabilities, risk environment, or resource availability. However, common characteristics can generally describe SLTT critical infrastructure programs in terms of their location, staffing, priorities, and primary focus areas. Figure 1 provides a high-level, nationwide snapshot of management and staffing factors, with additional detail on the common characteristics included in the following sections.

Figure 1. SLTT Critical Infrastructure Program Snapshot



Concerns about sustaining program operations contribute to decisions about program management, staffing, and priorities, particularly in light of reduced Homeland Security Grant Program funding nationwide, loss of Urban Areas Security Initiative (UASI) status for many jurisdictions, and constraints on SLTT government budgets for competing priorities. As detailed in Chapter 3. Risk Management, critical infrastructure programs aim to focus on high-priority risk management activities, but require funding and personnel for implementation. Specifically, dedicated resources are needed for core program functions, such as conducting risk assessments and private sector outreach, expanding training and exercise opportunities, and building cybersecurity program capabilities. While many programs have turned to the DHS Protective Security Advisors (PSAs) for assistance with these functions, long-term sustainability of the program and core activities is desired.

Location

The organizational location of the SLTT critical infrastructure program significantly impacts the mission and unique program focus areas. For instance, many programs are either located within fusion centers or maintain strong fusion center engagement, contributing to a major focus on information sharing that underlies such program activities as sharing threat information with sector partners. Over time, State programs have shifted from single mission support (e.g., exclusively supported by emergency management) to joint mission support (e.g., supported by both emergency management and homeland security agencies) or to fusion centers and homeland security agencies, where programs are guided by the nature of the all-hazards mission of their home organization. In addition, many State programs are becoming more formalized and are located at the department level. Formal, department-level programs not only increase visibility for their program, but this recognized location also facilitates collaboration, coordination, and connection to time-tested relationships across other State sector-specific agencies, as well as to Federal and local agencies and the private sector.

Staffing

SLTT critical infrastructure programs are typically staffed by SLTT government personnel rather than private contractors; however, the number of staff and their specific activities varies widely between jurisdictions. Many programs employ critical infrastructure directors or coordinators, who often maintain additional responsibilities, depending on their organizational location (e.g., managing broader homeland security, emergency management, and/or fusion center activities or agencies).

More advanced and long-standing programs (typically for States and regions with multiple major metropolitan areas) generally employ several dedicated personnel, including experienced critical infrastructure directors. Minimally-staffed programs (typically for fledging programs or jurisdictions with lower population density) have comparatively few, part-time personnel. Often, these programs manage additional priorities that compete for already scarce resources. In addition to directors and coordinators, common SLTT program personnel include planners, who focus on developing and implementing strategic documents, and analysts that identify critical infrastructure, conduct risk and threat assessments, and analyze risk information.

Priorities and Primary Focus Areas

Priorities of SLTT critical infrastructure programs are driven primarily by lifeline sectors, economic drivers critical to their jurisdictions, threat information, mass gathering and special events, and dependencies and cascading effects among sectors. Currently, common constraints that affect these priorities include cybersecurity risks, increased frequency of extreme weather events, prevalence of mass gathering events, evolution of threats to soft targets, aging infrastructure, local and private sector risk management needs, and requirements from Federal and State agencies.

Critical elements of critical infrastructure programs, consistent with NIPP 2013 Core Tenets, include implementing a partnership approach to security and resilience, sharing information with partners, and ensuring coordinated, comprehensive risk identification and management. Primary activities of critical infrastructure programs, consistent with NIPP 2013 risk management framework, include identifying infrastructure, assessing and analyzing risk, and setting goals and objectives.

- **Identify Infrastructure:** Though some programs have a relatively long history of identifying and assessing critical infrastructure, near-term priorities change with the risk environment in which new, emerging threats influence the focus on types of infrastructure to identify and assess.
- **Assess and Analyze Risk:** SLTT critical infrastructure assessment is a collaborative effort among SLTT government, fusion center, and DHS IP personnel, with PSAs as highly valued and relied-upon sources of support.
- **Set Goals and Objectives:** The majority of State programs have formalized their program strategies by either developing stand-alone critical infrastructure strategic plans (often modeled after national critical infrastructure policies and plans) or incorporating critical infrastructure elements into an overarching homeland security strategy. Either approach requires periodic updating.

Additional information on these and other risk management activities is included in Chapter 3. Risk Management.

2.2 Assets

SLTT critical infrastructure consists of assets, systems, and networks composed of human, physical, and cyber components. The security and resilience of these components are addressed by the specific risk management methodologies implemented by the SLTT owners and operators, with assistance from SLTT critical infrastructure programs.

Human assets are very important components of SLTT critical infrastructure, including millions of career and volunteer SLTT practitioners that actively serve in every community in the United States. In addition, several sectors contain significant SLTT portions of owners and operators. Though there are notable SLTT physical and cyber assets included in these sectors, as outlined in each sector's SSP, the activities of the people operating and managing such assets are what provide for the security and resilience of SLTT critical infrastructure. SLTT critical infrastructure programs rely heavily on information sharing among these sectors in order to perform their overall responsibility for safety and security within their jurisdictions.

Below is a summary of the SLTT-owned and operated assets for eight critical infrastructure sectors:

Communications

SLTT governments own, operate, and rely on a wide array of communications systems and equipment, especially for emergency response and recovery efforts. Key examples include public alert systems, 9-1-1 centers, emergency operations centers, and associated equipment. Specific radio frequency spectrum bands (e.g., 400 and 800 megahertz), upon which many Emergency Services Sector communications operations rely, are often only available to SLTT governments. In addition, public and private sector communications assets are frequently co-located (e.g., privately owned communication towers may grant space to SLTT equipment). The coordination of such critical communications systems and equipment requires a great deal of coordination among public and private sector stakeholders.

Dams

Approximately 25 percent of Dams Sector infrastructure is owned and operated by SLTT governments, including thousands of small and medium sized dams dispersed throughout the Nation. Select regions and critical industries depend heavily on these assets for hydroelectric power, nuclear plant cooling water, water storage, and protection from catastrophic flooding.

Emergency Services

A majority of Emergency Services Sector personnel are SLTT government employees and volunteers, including the disciplines of Emergency Management, Emergency Medical Services, Fire and Rescue Service, Law Enforcement, and Public Works. SLTT Emergency Services Sector operations provide the first line of defense for nearly all critical infrastructure sectors and the American public during natural disasters and other physical emergencies.

Energy

SLTT government personnel operate public utilities for electricity and natural gas. State public utility commissions regulate utilities at the State level and are engaged in a variety of critical infrastructure activities (e.g., cost-recovery, energy supply curtailment plans, emergency response, and cybersecurity). Local governments comprise a large set of Energy Sector stakeholders, representing the interests of cities, towns, and municipalities in sector security, protection, and emergency preparedness. Tribal agencies play significant roles in electricity transmission corridors, especially in the Southwest, and in various energy supply resources, including coal and potentially the growth of wind and other renewable energy sources.

Government Facilities

Govt Facilities

SLTT government facilities, including educational facilities, are a major component of the sector. Office buildings and government support facilities (e.g., for storage and maintenance of physical and cyber assets) are naturally critical to the secure operation of SLTT governments. Public education facilities (e.g., K–12 schools and public universities) are a very important part of American society overall.

Healthcare and Public Health

Healthcare

Public health departments and agencies are a critical portion of the sector, including SLTT components: millions of healthcare personnel, more than 1,000 hospitals, hundreds of thousands of ambulatory services, thousands of nursing and residential care facilities, and State health insurers. Public health personnel and agencies are often the first responders to health emergencies (e.g., pandemics and infectious diseases) and are therefore actively engaged in health preparedness and response for the American public.

Transportation Systems

Transportation Systems

A considerable portion of the Nation's transportation infrastructure is owned and operated by SLTT governments, including highways, roads, bridges, railways, airports, and inland navigable waterways. These jurisdictions are well positioned to address specific transportation security needs and preparedness and response capabilities. In addition to providing safe transport of people and commerce, SLTT departments of transportation are intricately involved in disaster preparedness, response, recovery, and mitigation with other critical infrastructure sectors (e.g., coordinating response fleet movements across jurisdictions and providing situational awareness of transportation capabilities) and in adaptation planning (e.g., conducting vulnerability assessments on climate impacts and adopting adaptation strategies).

Water and Wastewater Systems

Water

Public water utilities are operated by SLTT personnel, supporting and managing more than 150,000 public water systems (for drinking water) and more than 16,000 publicly owned treatment works (for wastewater) in the United States. These critical SLTT personnel are deeply integrated into the security and resilience of this lifeline sector and are therefore very important contributors to the security and resilience of other interconnected, interdependent sectors.

2.3 Risks

Critical infrastructure owned or operated by SLTT governments, or for which SLTT governments are responsible, face risks from multiple sources. Below are seven significant risk areas—encompassing threats and vulnerabilities and their associated risks—including the ability of SLTT governments to ensure security and resilience in their jurisdiction. These risks develop from the complexity of managing all hazards, resource limitations, and the lack of knowledge or awareness of critical infrastructure issues, tools, and programs. Additional sector-specific risks are detailed in each sector's 2015 SSP.

Physical Threats

SLTT governments are continually threatened by physical attacks on their critical infrastructure. High profile SLTT government facilities, services, and systems are frequent targets of those who wish to harm, impede, or sabotage government in general, or to steal government property. Public utilities may be targeted for extensive detrimental effect. The widespread increased use of unmanned aircraft presents an emerging risk, as these vehicles may be able to surpass common, established security systems. Emergency operations centers are physically connected to SLTT and private sector resources, which may be targeted to hinder emergency response and recovery efforts. Similarly, dependencies and interdependencies among SLTT and private sector critical infrastructure may be exploited.

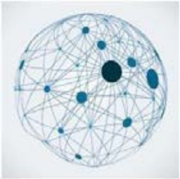
Cyber Threats

Cyber threats (e.g., phishing attempts, hacking incidents, and outdated software) are a constant and ever-changing threat to cyber systems across a broad spectrum of sectors. Moreover, personnel throughout the sectors have varying degrees of cybersecurity knowledge and understanding of cyber threats and attack vectors. This is an area of growing concern for SLTT governments because of the pervasive dependence on cyber infrastructure within SLTT governments, as well as throughout the sectors. It is further complicated by the necessity of cybersecurity to go beyond securing stationary assets to securing mobile information systems needed during emergency response.

Natural Disaster Threats

Preparedness, response, recovery, and adaptation to natural disasters are primary functions of SLTT governments. As natural disasters and weather become more frequent or extreme, a timely response and recovery by government entities will become more challenging, taxing limited government resources.

Understanding Dependencies and Interdependencies



Understanding the dependencies and interdependencies within and across government jurisdictions is critical for continuity of operations should a disaster occur. Local disasters can spread to multiple jurisdictions and sectors, triggering impacts across larger geographic areas. SLTT governments need to work with all sectors in order to understand the cascading and escalating impacts of affected assets. Discovering and fully understanding sector and system dependencies and interdependencies can be complicated due to information-sharing silos, lack of two-way information flows, or inadequate opportunities for or awareness of exercises and training.

Prevalence of Mass Gathering Events

Venues and structures for large public gatherings are common across SLTT governments. However, mass gatherings also provide an ideal opportunity for those with harmful intent to potentially cause a great deal of damage to people and infrastructure. Active shooter events and violent extremism (e.g., domestic terrorism) are of growing concern to SLTT governments responsible for the safety and security of their citizens and first responders.

Resource Constraints

The continuity of SLTT critical infrastructure programs and activities is constantly hindered by limited and diminishing resources (especially for maintaining dedicated program personnel), predominately a result of losing Federal grant funding. This forces SLTT governments to focus on highest-priority activities and restricts governments to being reactive rather than proactive. Program continuity is also threatened by the turnover of personnel (e.g., from changing SLTT administrations), including those at the Federal level, which leads to loss of local knowledge. In addition, resource constraints limit the capacity for SLTT programs to address the expansive portfolio of assets within a jurisdiction.

Partnership Development Constraints

Public-private partnerships are essential to facilitate and enable planning and preparedness for critical infrastructure security and resilience. Major challenges to sustaining public-private partnerships include time, resources, and personnel constraints limiting partnership outreach; the need to consistently deliver products and events that are highly-valued by partners to secure consistent participation; and time between disasters leading to diminished participation (due to a sense of complacency). In addition, information security concerns and bidirectional information-sharing prohibitions may impact the flow of critical information to ensure full public and private sector knowledge of risks, capabilities, and mitigation efforts.

2.4 Key Partnerships

Incidents do not respect jurisdictional or organizational lines, making partnerships a key contributor to security and resilience at the local, regional, and national levels. The NIPP 2013 recognizes the important role of partnerships in partner collaboration, information sharing, education and awareness, and emergency response across sectors and jurisdictions. Partnerships leveraged by SLTT critical infrastructure programs include regional partnerships and cross-sector or sector-specific partnerships that serve strategic or operational purposes. In addition, the SLTTGCC operates at the national level to collaborate between jurisdictions and with the Federal Government.

While membership demographics, governance structure (e.g., non-profit, funding by a government agency), and specific activities vary, regional partnerships share an underlying focus on public-private partnership development. Membership often extends beyond the typical government and infrastructure owner/operator base to reach partners largely different from those of national partnerships (e.g., emergency management professionals, small- and medium-sized businesses, non-profits, community groups, Voluntary Organizations Active in Disasters, educational institutions, and other local or regional private sector leaders). Primarily operational, these partnerships continually provide their members with an extended network of government and industry partners to identify and address emerging critical infrastructure security and preparedness issues facing the region.

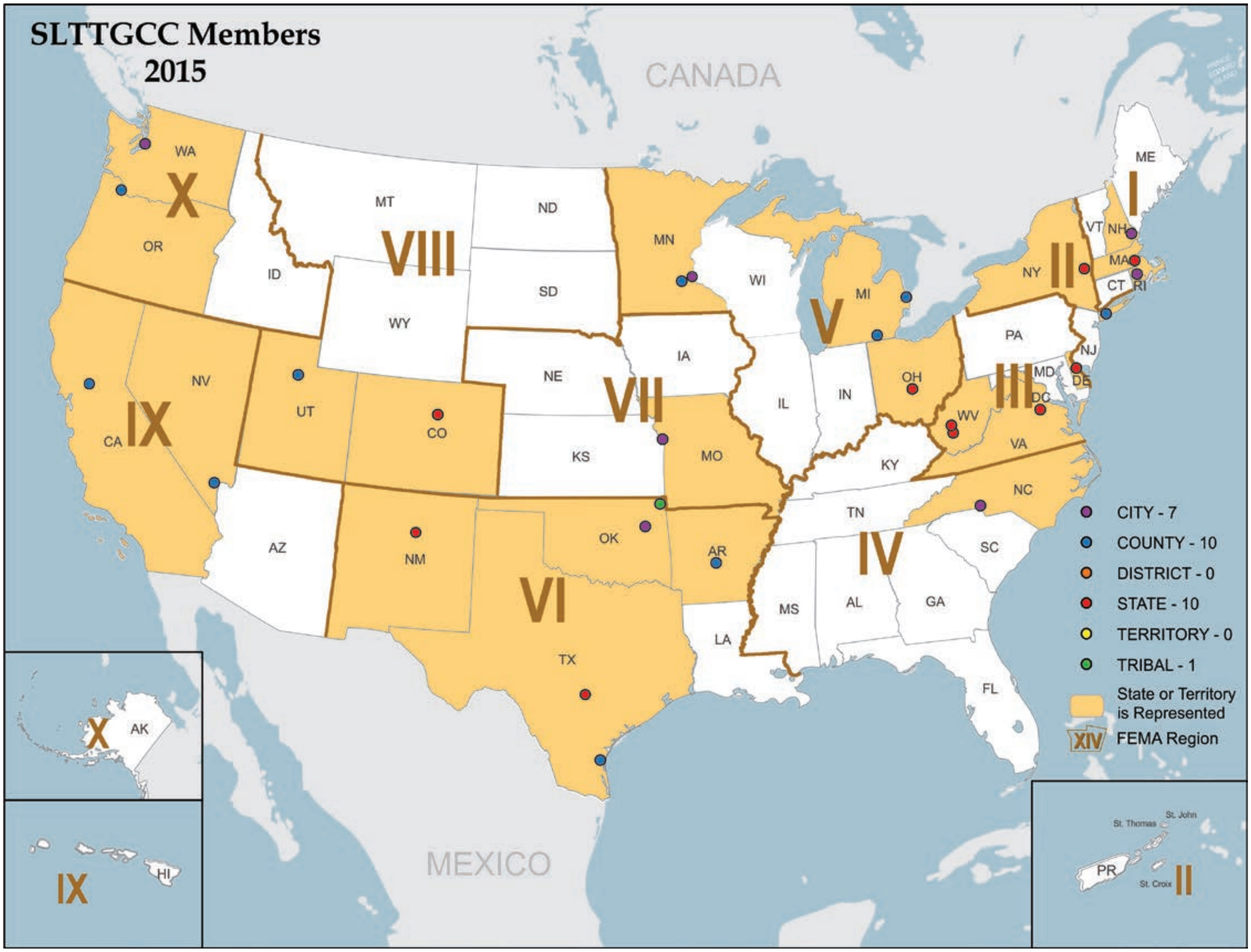
SLTT critical infrastructure programs establish or join strategic or operational formal cross-sector or sector-specific partnerships to cultivate stakeholder relationships through high-valued activities (e.g., planning, training, and exercises), leverage expertise, understand assets and interdependencies, and share best practices. Lifeline sectors (e.g., Energy, Communications, Transportation Systems, and Water and Wastewater Systems), sectors with the greatest economic impact to the region (e.g., Financial Services, Commercial Facilities, and Chemical), and public safety sectors (e.g., Emergency Services) are most often represented in formal partnerships. SLTT programs also directly engage private-sector partners in these and other sectors and leverage established partnerships—including Local Emergency Planning Committees (LEPCs), Area Maritime Security Committees, and InfraGard Chapters—as force multipliers to collaborate regionally, build relationships and trust, and better connect infrastructure security and emergency management missions.

At the national level, the SLTTGCC provides the organizational structure to strategically coordinate with multiple stakeholders—including across jurisdictions and disciplines, with DHS, and with other NIPP 2013 partnership councils. Facilitating senior-level strategic communications and coordination on SLTT agency initiatives, activities, and best practices enables the Council to take a central role in security and resilience and educate others on implementation of the NIPP 2013. Working directly with DHS enables the Council to meaningfully contribute to the improvement of Federal critical infrastructure programs, tools, and capabilities utilized by SLTT agencies, including those offered by the PSAs. SLTTGCC collaboration with the other cross-sector partnerships identified in the NIPP—including the Federal Senior Leadership Council, Critical Infrastructure Cross-Sector Council, and RC3—supports efforts to plan, implement, and execute the Nation's critical infrastructure security and resilience mission. The following examples highlight accomplishments of this collaboration:

- The SLTTGCC **Sector Liaison Program** enables councilmembers to participate actively in SCC meetings to share SLTT perspectives, participate in policy discussions, contribute to SSP development, and maintain communication between the SLTTGCC and the critical infrastructure sectors.
- Monthly conference calls with the **National Council of Information Sharing and Analysis Centers (ISACs)** allow SLTTGCC leadership to provide updates on Council activities and member initiatives. This visibility on efforts expands the Council's network and contributes the SLTT perspective on important information-sharing efforts.
- **DHS Regional Directors (RDs) and PSAs** are integral to the success of many critical infrastructure programs and are valuable partners to the SLTTGCC in jointly collaborating on assessment tools, training and exercises, and information sharing. The Council has included RDs and PSAs in many plenary sessions to facilitate discussion on the use and effectiveness of Federal critical infrastructure programs and activities.
- During 2015–2016, the SLTTGCC is collaborating with the **RC3** to sponsor the Regional Overview of Critical Infrastructure Programs project to document the current state of the critical infrastructure mission implementation across the Nation. By engaging SLTT personnel and public-private partnerships, the Councils are summarizing operational and budgetary changes over time, detailing activities, and facilitating the sharing of information and best practices.

Figure 2 provides a visual representation of the Council's membership spanning the country. An updated list of SLTTGCC members and working groups can be found at http://www.dhs.gov/sltt-gcc.

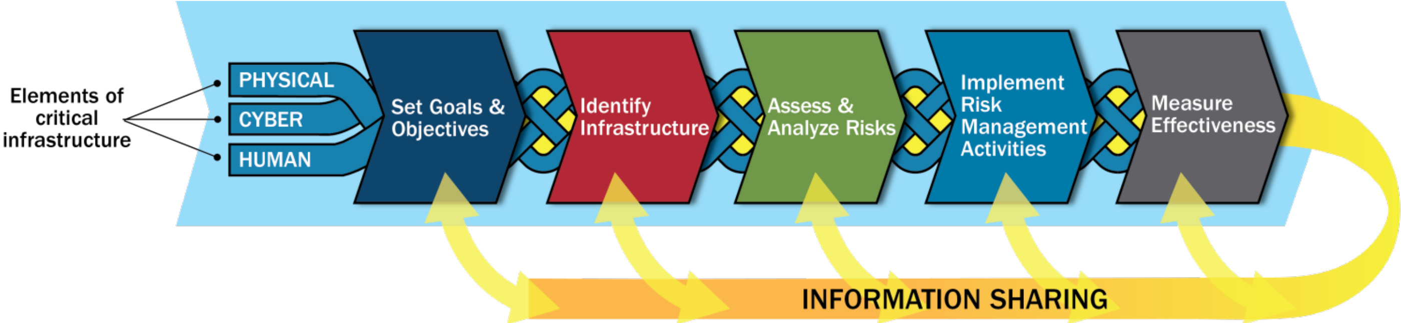
Figure 2. SLTTGCC Membership Map (as of July 2015)



3. RISK MANAGEMENT

Risk management is a cornerstone of the national effort to strengthen critical infrastructure security and resilience and is relevant at all levels of government. Vital to this national effort are SLTT government agencies that manage a wide-range of risks through their critical infrastructure programs and activities. Their ability to make risk-informed decisions on the most effective solutions in both steady-state and crisis operations is important to ensuring security and resilience and reinforces the Nation's economic, public health, and national security. Risk is the potential for an unwanted outcome resulting from an incident determined by likelihood and associated consequences. Risk management is an approach to making and implementing informed security and resilience decisions for physical, cyber, and human elements of critical infrastructure. As outlined in the NIPP 2013 and depicted in Figure 3, collaborating to managing risk includes five primary functions, each supported by a feedback loop facilitated by information sharing.

Figure 3. NIPP 2013 Risk Management Framework



This chapter describes the wide variety of SLTT activities employed by SLTT critical infrastructure programs to mitigate risk in a manner that is consistent with the jurisdiction's unique risk profile and resource availability. Further, it summarizes the most common significant topical critical infrastructure risk areas facing SLTT governments and prevention/mitigation efforts (e.g., cybersecurity, mass gatherings, dependencies, and large-scale incidents), and highlights potential risk management activities of SLTT agencies that can be implemented in the future depending on authorities, personnel, and resource availability.

3.1 Risk Management Landscape and Activities

To manage the risks from significant threats and hazards to physical and cyber critical infrastructure, SLTT government agencies embrace an integrated approach encompassing diverse public and private sector partners and conduct a variety of risk management activities. Across the Nation, SLTT critical infrastructure programs construct different priorities depending on the risk environment, underlying constraints, and risk tolerance. Risk tolerances can vary greatly, depending on jurisdiction, organizational structure, resources, regulatory environments, and infrastructure criticality and dependencies.

SLTT government agencies implement risk management activities consistent with the NIPP 2013 risk management framework, with some agencies using the framework as a constructive model to orient SLTT security plans and resilience strategies. As each jurisdiction manages their security and resilience responsibilities differently, it is important that the critical infrastructure program management processes support the responsibilities as defined in the NIPP 2013 and specific to their area of responsibility.

Set Infrastructure Goals and Objectives

In support of the National Preparedness Goal and the strategic direction on which critical infrastructure activities should be focused, SLTT agencies identify objectives and priorities for programs and scale them to their operational and risk environments and resources. This enables the construction of programs responsive to SLTT needs and reflective of the area of responsibility in which these programs operate, but aligned with national priorities and goals and sector objectives. Although nearly all SLTT agencies construct security and resilience goals and objectives aligned with national goals and priorities and public and private sector objectives, they vary in approach. The SLTT process for setting infrastructure goals and objectives includes fundamental features:

- **Formalized Programs and Plans:** SLTT agencies establish formal programs with a critical infrastructure coordinator/manager and develop strategic plans that are structured as a standalone plan or built into a homeland security or emergency management strategy. Common plan elements include topical focus areas (e.g., jurisdiction-specific sectors of importance and enhancing cybersecurity awareness), asset identification and management, information sharing, building partnerships, and risk management program activities (e.g., training, exercises, and infrastructure assessments). States may formalize plans to provide a standard for local plans, provide templates and program technical assistance, or incorporate plan and program ideas from other States. Some programs/plans decentralize critical infrastructure program implementation—shifting responsibility from the State to the local or regional level.

- **Joint Planning Efforts:** In support of all-hazards missions, SLTT agencies incorporate various localities and disciplines (e.g., homeland security, emergency management, emergency services, intelligence, and sector-specific disciplines) into their planning efforts. This includes building cross-agency relationships, establishing diverse working groups (e.g., through public-private homeland security advisory councils), building multidisciplinary strategy and assessment teams, or co-locating with or detailing personnel to another agency (often integrating fusion center capabilities and personnel into critical infrastructure planning).
- **Continual Evaluation:** SLTT agencies continually reevaluate goals to ensure they remain effective, are responsive to their jurisdiction's unique risk environment and resource constraints, and support national goals and priorities.

Identify Infrastructure

Critical infrastructure risk management cannot be achieved without first identifying the critical assets, systems, and networks and understanding their dependencies and interdependencies. SLTT agencies may view infrastructure criticality differently, based on their unique risk environment. However, all agencies recognize the importance of a modern system or program to collect data to achieve risk-informed decision-making. SLTT agencies use asset identification and collection tools and leverage partnerships to contribute to the management of physical, cyber, and human assets. The following resources allow SLTT agencies to identify, gather, validate, and update pertinent information on critical assets, systems, and networks:

- **IP Gateway:** Used to input and retrieve critical infrastructure information, IP Gateway also enables comprehensive vulnerability and risk analysis through the Infrastructure Survey Tool and other assessments, analytical products, and reports.
- **PSA Program:** PSAs collaborate with SLTT agencies and private sector owners and operators to identify critical infrastructure significant at various government levels and update associated inventories. PSA tools such as the Enhanced Critical Infrastructure Protection (ECIP) visits, Infrastructure Survey Tool, and Rapid Survey Tool inform the collaborative process.
- **Partnerships and Liaisons:** SLTT agencies utilize existing liaisons, partnerships, and councils to leverage the knowledge of public and private sector subject matter experts to identify assets. This may include developing private sector outreach initiatives or liaisons participating in regional tasks forces.
- **National Critical Infrastructure Prioritization Program (NCIPP) Data Call:** The NCIPP Data Call is the basis for creating the national prioritized infrastructure list and includes coordination among UASI jurisdictions, government councils, State agencies, private sector owners and operators, and PSAs. NCIPP infrastructure nominations must meet minimum specified consequence thresholds.
- **State Data Calls:** To facilitate a robust asset identification process, State critical infrastructure programs host data calls with other State agencies, local agencies, regional organizations, and the private sector to identify critical infrastructure in their respective area of responsibility. Infrastructure criticality is based on potential significant impacts (e.g., economic losses, fatalities, interdependencies) at the local, regional, and State level.
- **DHS Special Events Working Group:** With an increasing focus by SLTT critical infrastructure programs on special events, this single forum aids preparedness and response by ensuring comprehensive and coordinated awareness of, and appropriate Federal support to, special events. Specifically, the working group provides a means to identify, categorize, and rank events that could have a cascading effect on people, property, resources, and the environment.
- **Geographic Information System (GIS) and Mapping Tools:** An increasing number of SLTT agencies are utilizing GIS tools to provide a comprehensive picture of critical infrastructure in their area of responsibility. Mapping critical infrastructure and dependencies contributes to effective risk management and supports SLTT agencies in identifying lifeline functions and preparedness planning and capability development. These GIS tools are informed by unique data sets such as identified hazards, facility locations, transportation systems, soft targets (e.g., schools), historical data, and nearby emergency services operations.

In addition to identifying critical infrastructure, SLTT agencies seek to identify dependencies, interdependencies, and cascading effects in order to comprehend the consequences of a disruption or attack on an asset, system, or network. To accomplish the identification of dependencies, SLTT agencies significantly engage in information sharing with stakeholders across the critical infrastructure community, in addition to building relationships and partnerships across disciplines and jurisdictions. Agencies may also use exercises and trainings to identify key lifeline sector dependencies.

Assess and Analyze Risks

Critical infrastructure risk is assessed in terms of threat, vulnerability, and consequence. SLTT agencies perform critical infrastructure risk assessments to inform their risk management program decision-making using a broad range of methodologies (e.g., THIRA and onsite threat assessments). To fully understand the risk environment, SLTT agencies utilize comprehensive risk assessment methodologies. SLTT agencies also perform specific-purpose risk assessments, such as threat, vulnerability, and consequence assessments to better understand specific components of risk. To effectively assess risk, SLTT agencies rely on timely, reliable, and actionable information regarding threats, vulnerabilities, and consequences. A key element to assessing and analyzing risks is that non-governmental entities are engaged in a trusted environment, where they are involved in the development and dissemination of products regarding threats, vulnerabilities, and potential consequences. The following risk assessment tools support comprehensive SLTT risk management decision-making. These tools are commonly leveraged to assess and analyze prevalent SLTT risks relating to physical, cyber, and natural disaster threats; dependencies and interdependencies; mass gathering events; and constraints of resources and partnership development.

- **SLTT Hazard Identification and Risk Assessment (HIRA):** SLTT agencies conduct HIRAs to understand and examine specific potential or existing circumstances that can generate a disaster or emergency incident at the SLTT level. HIRAs focus on the quantitative assessment of hazards and consequences.
- **THIRA:** Expands on HIRAs by broadening what is considered throughout the risk assessment process. SLTT agencies use the THIRA process to complete qualitative risk assessments steps: identify the threats and hazards of primary concern to the community, develop threat and hazard context, establish targets for each core capability within the National Preparedness Goal, and apply the results to estimate resources required.
- **ECIP:** Facilitates outreach to establish or enhance relationships between DHS and owners and operators. Voluntary security surveys are offered as a result of the outreach and are conducted by DHS PSAs to assess the overall security and resilience of prioritized critical infrastructure sites.
- **RRAP:** A cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. Federal, SLTT, and private sector stakeholders collaborate on threat, vulnerability, and consequence all-hazards risk assessments and an analysis of infrastructure dependencies and interdependencies. Each RRAP project typically involves a year-long data collection and analytical effort followed by continued collaboration of regional stakeholders to support resilience.
- **Onsite Assessments:** SLTT agencies deploy onsite risk assessment teams that focus on prioritized assets within their area of responsibility. Many risk assessment teams concentrate on critical infrastructure vulnerability and provide recommendations to the owner or operator to address potential threats and security vulnerabilities. These teams can incorporate multiple disciplines, mission areas (e.g., homeland security), and jurisdictions, or can comprise dedicated SLTT personnel from the same critical infrastructure program.
- **Planning Efforts:** Joint committees, such as LEPCs, primarily comprise local emergency services representatives familiar with a variety of jurisdiction-specific risk factors. LEPC meetings are open to all emergency management stakeholders and enable the illumination of risk factors that may be inadvertently excluded from assessments.
- **Cybersecurity Assessments:** To assess cyber risk, SLTT agencies utilize cybersecurity tools offered by DHS, such as the Cybersecurity Assessment and Risk Management Approach, Cyber Resilience Review, and the Cyber Security Evaluation Tool. These cybersecurity tools provide a picture of sector-wide cyber risks, evaluate operational resilience and cybersecurity practices, and assess the cybersecurity posture of industrial control systems. In addition, SLTT agencies leverage DHS Cyber Security Advisor assessment tools, with some agencies using DHS cybersecurity tools to provide assessments to external agencies, such as local governments.
- **Analytic Tools and Products:** Analytic tools—such as risk management decision support systems—enable real-time monitoring of hazards, in addition to early warning dissemination. This produces enhanced situational awareness and leads to better resilience planning, such as in flooding preparedness for transportation systems. To assess risk effectively, SLTT agencies utilize the outputs from various assessments and leverage analytic products

from a variety of agencies at all levels of government (e.g., DHS Office of Intelligence and Analysis (I&A)). In addition, State agencies share these analytic products, as appropriate, with stakeholders across the critical infrastructure community to contribute to an overall mission of infrastructure security and resilience.

The following information represents the risk assessments designed to address a specific component of risk (threat, vulnerability, or consequence) to inform risk management decisions:

- **Assessing Threats:** A threat is defined as the natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. When assessing risk, the threat of an intentional hazard is estimated as the likelihood of an attack that accounts for both the intent and capability of the adversary. Threat assessments are the most frequent type of specific-purpose assessment utilized by SLTT agencies. In assessing threats, agencies consider the full spectrum of intentional and unintentional threat sources, including natural hazards (e.g., hurricane, fire, pandemics), technological hazards (e.g., power failure, train derailment, radiological release), and human-caused incidents (e.g., biological attack, cyber incident, sabotage). SLTT agencies recognize that threat assessments are most effective when applied to a specific geographic region, State, or locality, and threat source. Primary threat assessments include:
    - **SLTT Fusion Center Threat Assessments:** Many SLTT critical infrastructure programs are located within fusion centers or maintain strong fusion center engagement, enabling these programs to easily leverage fusion center and law enforcement-generated threat assessments and analyses. Fusion centers combine timely threat information with risk information (e.g., identified hazards, historical risk); thus enabling SLTT agencies to effectively manage their security posture. Threat assessment resources may take the form of regular conference calls with private sector liaisons, sector-specific bulletins, or in-depth topical threat reports.
    - **Federal Threat Assessments:** SLTT agencies also utilize threat information and analysis from the Federal Government, including the National Infrastructure Simulation and Analysis Center, Office of Cyber and Infrastructure Analysis, DHS I&A, and the Federal Bureau of Investigation (FBI). Information-sharing portals, such as the DHS Homeland Security Information Network (HSIN) and the FBI's Guardian Program, are leveraged as mechanisms to share threat-related information with vetted homeland security professionals and facilitate threat reporting and collaborating.
- **Assessing Vulnerabilities:** A vulnerability is defined as the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. SLTT agencies leverage ECIP outreach and surveys—including the Infrastructure Survey Tool, Rapid Survey Tool, and Computer-Based Assessment Tool—to assess vulnerabilities.
- **Assessing Consequences:** A consequence is defined as the effect of an event, incident, or occurrence that reflects the level, duration, and nature of the loss resulting from the incident. Common consequences SLTT agencies seek to understand include public health and safety, economic, psychological, and governance or mission impact.

Implement Risk Management Activities

Risk management activities are the cornerstone of SLTT critical infrastructure programs. By systematically conducting risk assessments to assess SLTT assets, systems, and networks, SLTT agencies are able to make informed decisions and increase the defensibility of resource allocation decisions. Agencies may prioritize risk management activities based on various elements, such as activity costs, potential for risk reduction, and varying levels of infrastructure criticality. All elements are shaped by the different views across jurisdictions and the unique risk environment. The following summarizes the activities SLTT agencies most often conduct in pursuit of specific functions: identify, deter, detect, disrupt, and prepare for threats and hazards; reduce vulnerabilities; and mitigate consequences:

- **Assessments:** SLTT agencies conduct a variety of assessments depending on the threat environment and are increasingly requested to conduct soft target security surveys and provide options for consideration to increase the site's security posture. Assessments can range from comprehensive (e.g., inclusive of threat, vulnerability, consequence, and dependencies) to specific purpose (e.g., threat).
- **Training and Exercises:** SLTT agencies not only undergo regular training to improve security capabilities (e.g., active shooter incident response), but they also sponsor robust training programs designed to improve the capabilities of public and private sector stakeholders. Trainings and exercises are typically conducted onsite; however, FEMA's Emergency Management Institute and public-private partnerships offer online critical infrastructure training. The most commonly deployed topical trainings and exercises include cybersecurity,

active shooter, and natural hazard incidents, particularly when exercising expansive events across jurisdictional boundaries.

- **Partnerships:** Ensuring security and resilience requires an engaged whole community—Federal and SLTT governments, owners and operators, regional entities, non-profit organizations, and academia. SLTT agencies recognize the criticality of partnerships and continually make them a cornerstone of their programs. Partnerships provide subject matter experts, training programs, educational opportunities, information-sharing mechanisms, and a connection to the private sector.
- **Information Sharing:** Information sharing underlies all components of the risk management framework, facilitates collaborative problem solving, and is critical to a common operating picture, particularly during expanding incidents or incidents that affect multiple jurisdictions simultaneously. Information-sharing mechanisms used by SLTT agencies to share information with public and private sector partners include:
  - **Secure Access Portals:** SLTT agencies use HSIN portals and TRIP*wire* (Technical Resource for Incident Prevention) to receive key analysis and to collect, analyze, and disseminate information to vetted partners. Agencies may also utilize other Federal resources, such as the FBI Guardian system. Public-facing SLTT agency Websites are also relied upon heavily.
  - **Bulletins and Newsletters:** These information products include regular sector-specific or topical open-source reports; newsletters containing upcoming projects, best practices, or achievements; and bulletins or reports forwarded from other entities (e.g., DHS Office of Cyber and Infrastructure Analysis Critical Infrastructure Security and Resilience Notes).
  - **Briefings:** SLTT agencies regularly conduct briefings to inform their leadership of program activity, improvement, and strategy; disseminate information with various sectors; share best practices; and communicate threat information and adversary tactics. Briefings are conducted in-person, on conference calls and Webinars, or during conferences (e.g., National Homeland Security Conference).
  - **Fusion Centers:** Many SLTT critical infrastructure programs are integrated with SLTT fusion centers and have strong engagement with fusion centers on activities with a critical infrastructure nexus. Fusion centers deliver wide-ranging intelligence products (e.g., joint intelligence products); provide an accessible hub to homeland security activity and partnerships (i.e., DHS, FBI, or fusion liaison programs); and offer resources to improve homeland security capabilities such as trainings, Webinars, or toolkits.
  - **Conferences:** SLTT agencies host and attend conferences to share best practices, promote threat and hazard awareness, achieve critical infrastructure activity situational awareness, and network with subject matter experts and the critical infrastructure community. Conferences also provide educational opportunities for critical topics, such as cybersecurity.
  - **Partnerships:** Public-private partnership organizations (e.g., InfraGard); government and private sector councils, working groups, and task forces; ISACs; academic institutions; and interagency relationships provide unique opportunities for two-way information sharing on hazards, threats, sector interdependencies, and best practices.

Measure Effectiveness

Measurement efforts are an important step in the risk management process and facilitate the determination of effective investments, programs, and activities. Although not yet widely integrated throughout all SLTT critical infrastructure programs, some SLTT agencies use a variety of indicators to measure the efficacy and continuous improvement of their security and resilience risk management activities. Performance measurement effort activities include reviewing program goals and tracking implementation, developing metrics for conducting assessments and follow-up visits, measuring outcomes related to capability targets identified through the jurisdiction's THIRA and State Preparedness Report, disseminating information products complete with a feedback form, hosting formal and informal discussions with sector partners on activity effectiveness, and conducting exercise after-action activities (e.g., hot wash) to share strengths and areas for improvement.

3.2 Managing for Security and Resilience: Common Significant Risks

In managing for critical infrastructure security and resilience, SLTT agencies embrace an all-hazards approach. However, the environment in which each SLTT agency operates can vary with geography, mission, prioritized risk areas, infrastructure criticality, and resource constraints. Although SLTT agencies structure their critical infrastructure programs to address all-hazards, common program focus areas seek to prevent or mitigate risk. The information below represents the most common significant risk areas that SLTT agencies manage to ensure security and resilience in their area of responsibility. Considering the frequency of these risk areas across various jurisdictions, these areas can also be recognized at the national level.

Cyber

The cybersecurity issue is exceedingly complex. To manage cyber risk, SLTT agencies consider a multitude of issues, many of which are classified as "unknowns" or are subject to knowledge deficiencies. In addition, the interpretation of cybersecurity resilience varies among agencies. Although the cyber risk environment is individualized based on each entity's security capabilities and infrastructure vulnerabilities, common cybersecurity issues are repeated across jurisdictions. These include cyber-physical system dependencies, increasing dependence on technology, potential cyber vulnerability exploitation by nefarious actors, access control, information security deficiencies, and personnel and knowledge gaps. Two of the major cyber risk areas SLTT agencies focus on are information security and infrastructure system access control. Managing and securing the complex collection of personal, consumer, and financial information and controlling the access to that information and infrastructure are seen as priorities for both governments and businesses alike.

In many cases, because of the complexity of system dependencies and magnitude of unknowns, the impact of a cyber incident expands beyond the initial target and generates impacts to agencies dependent on the compromised infrastructure. Containing the expansion of attack impact may also be complicated by information-sharing barriers and the evolving nature of cyberattack vectors (e.g., information security breaches, hacking, phishing, and malware). Successfully securing cyber systems relies on the timely sharing of information (e.g., threat, incident, and response capability) between public and private sector stakeholders.

Soft Targets

Soft targets are sites that are more vulnerable to attack—compared to hardened facilities—due to their open access and limited security barriers. Soft targets include banks, shopping malls, supermarkets, apartment buildings, schools and universities, churches, and places of recreation and entertainment. The vulnerability of soft targets is a growing concern due to the comparative ease at which perpetrators can compromise or execute an attack on these softer infrastructures and evade pre-operational detection—efforts which may be more difficult to execute on hardened facilities. The increasing number of special events and mass gatherings (e.g., open access sporting events, parades) are of particular concern to SLTT agencies that must prevent or mitigate risks in a densely populated and open-access area. Violent extremist threats from a range of violent extremist groups and individuals, including the domestic terrorist and homegrown violent extremist, further complicate the issue of soft target security. Increasingly sophisticated use of the Internet, social media, and information technology by actors with nefarious intent (e.g., violent extremists) adds an additional layer of complexity.

Dependencies

The security and resilience of the Nation is highly dependent on secure SLTT critical infrastructure operations. Therefore, the disruption of services and functions of SLTT critical infrastructure can produce consequences that quickly expand beyond the scope of the initial incident. For instance, when lifeline sector services (e.g., communications, energy, transportation, and water and wastewater) are compromised, the disruption negatively affects a wide range of communities dependent on the sector's operations—other sectors, various levels of government, public, and private sector companies—in addition to negatively impacting the Nation's public safety, security, and morale. In addition, much of the critical infrastructure primarily owned and operated at the SLTT level depend on each other to safely and securely operate in both steady-state and emergency situations. A failure in one sector could cascade to another and ignite an impact chain reaction that expands beyond the local level and affects supply chains at various levels (e.g., State, regional, national, and international).

The increasing age of critical infrastructure throughout the United States—including electrical grids, water and wastewater systems, and roads and bridges—increases the risk of failure and the magnitude of impacts due to infrastructure dependencies. This creates incidents that require SLTT response while also impeding services critical to SLTT functions. SLTT governments also frequently own and operate such infrastructure; thus the importance of their preparedness and response capabilities for failing infrastructure events is compounded.

Expansive Incidents

Across the entire spectrum of threats and hazards (e.g., natural, technological, and human-caused incidents), certain incidents concurrently or subsequently affect multiple jurisdictions. Natural disasters—the most common incidents that SLTT agencies manage—pose a unique risk to SLTT agencies responding to the incident. Frequent and extreme weather events can increase the response demands, which may drain sector personnel, assets, and capabilities and may also threaten key services that enable an SLTT response. In many cases, natural disasters are not localized and may impact an entire region's infrastructure, such as in the event of a major hurricane.

Whether resulting from acts of nature, failure or accident, or intentional acts from an adversary, expansive incidents (e.g., chemical, biological, or radiological) can expand beyond the local level and may affect a region or the Nation. For example, biological agents or infectious disease can quickly spread through numerous jurisdictions and greatly strain SLTT resources (especially local public health facilities, personnel, and supplies), impacting the health and safety of large numbers of the public and responders. The risk from such incidents is compounded by the challenge of containing incidents at the local level. The medical community (of which public health departments and agencies are critical components) and SLTT personnel must receive appropriate instruction and messaging on quarantine and isolation measures.

3.3 Risk Management Outlook

Across the Nation, SLTT agencies encounter various challenges in conducting risk management activities in pursuit of an all-hazards mission to secure and ensure the resilience of SLTT critical infrastructure. The information below represents the challenges and emerging risk management activities—comprising a risk management program activity outlook—that SLTT agencies seek to overcome and the activities to which agencies want to allocate future resources. The degree to which specific risk management activities are conducted by SLTT agencies is dependent on authorities, personnel, and resource availability.

- **Formal and Integrated Programs:** Although many SLTT critical infrastructure programs are formalized, some SLTT programs operate informally, and many programs are not integrated at a regional level. This proves a challenge to addressing infrastructure dependencies that cut across multiple sectors and jurisdictions, as well as coordinating program activities to reduce duplication.
- **Personnel:** Many SLTT critical infrastructure programs are understaffed, due to personnel shortages or turnover, and are overwhelmed by an expanding risk management activity portfolio. For example, SLTT programs can outline specific improvements to address capability gaps identified in the THIRA and State Preparedness Report, but ultimately require dedicated personnel to perform these critical activities. Such activities may include developing and administering private sector training on cybersecurity, hosting multi-jurisdictional exercises on natural disaster response, assessing infrastructure dependencies and cascading effects, or using advanced risk management technology (e.g., GIS and data layers) to assess critical infrastructure and model risk.
- **Private Sector Outreach:** Private sector engagement continues to be a key activity for ensuring public and private security and resilience. Offering private sector training and improving information sharing to and from the private sector would address major issues, such as sector dependencies and infrastructure resilience.
- **Credentialing:** SLTT personnel typically carry several different identification credentials in order to perform their routine duties, as well as operate effectively during emergencies. The demand for multiple types of data associated with individual credentials—such as identification, affiliation, certification, privilege, and authorization data—and the demand for how quickly credentials allow personnel to access incident sites is increasing. Addressing access control and credentialing challenges requires the advancement of credentialing from simple identification cards to the technologically advanced, multifaceted credentials currently available (e.g., those based on the Federal Personal Identity Verification Interoperability for Non-Federal Issuers standard).
- **Soft Target Security Surveys:** Increasingly, SLTT programs are receiving requests to conduct security surveys for soft targets (e.g., banks, shopping malls, supermarkets, and churches). As the violent extremist threat grows and expansive incidents (e.g., extreme weather) occur more frequently, so do survey requests from sites with which SLTT programs have not traditionally interacted.
- **Cybersecurity:** The complexity of cybersecurity is compounded by resource constraints, knowledge and training deficiencies, a public and private sector disconnect, and unidentified cyber-physical infrastructure dependencies. Also challenging is the discourse on the scope of public and private sector involvement in cyber incident investigations, cyber threat information sharing, and developing and implementing industry or national cybersecurity standards.

4. VISION, MISSION, GOALS, AND PRIORITIES

SLTTGCC VISION

Fully integrate State, local, tribal, and territorial governments in national critical infrastructure security and resilience efforts to ensure a safe, secure, and resilient infrastructure.

SLTTGCC MISSION

Coordinate and advocate State, local, tribal, and territorial government perspectives to the critical infrastructure community to facilitate collaboration across jurisdictions on SLTT government guidance, strategies, and programs and to help execute the Nation's critical infrastructure security and resilience mission.

4.1 SLTTGCC Goals and Priorities

The following SLTTGCC goals and priorities represent the Council's view of how best to support the five overarching goals of the NIPP 2013 and Joint National Priorities, and achieve a secure, protected, and resilient SLTT critical infrastructure community. Emphasizing the Council's requirements under the NIPP 2013, the Council's role in affecting change in the evolving critical infrastructure mission space, and collaboration with primary Council partners, the goals provide the framework to guide security and resilience efforts and improve SLTT government risk management practices. The priorities take into consideration the unique risk management perspectives and resources of SLTT agencies and focus on enduring capabilities that address critical infrastructure needs over the long term. A summary of how SLTTGCC goals and priorities contribute to the NIPP 2013 goals and Joint National Priorities is located in Appendix B.

Table 1. SLTTGCC Goals and Priorities

Goals		Priorities	
1	**GROW AND MATURE THE COUNCIL** Mature and become agile to meet NIPP 2013 requirements, accomplish goals and priorities, and effectively represent SLTT critical infrastructure perspectives.	PRIORITY A	Maintain a strategy to identify, recruit, and maintain balanced and representational membership.
		PRIORITY B	Identify, recruit, and maintain a cadre of critical infrastructure subject matter experts to participate in working groups.
		PRIORITY C	Identify, recruit, and maintain an Alliance Network of critical infrastructure professionals with which to network and share best practices.
		PRIORITY D	Maintain a Sector Liaison program between the SLTTGCC and the other GCCs and SCCs.

Goals	Priorities	
2 **INFORM THE CHANGING CRITICAL INFRASTRUCTURE LANDSCAPE** Identify and articulate changes in the SLTT critical infrastructure mission and educate others on operating within the changed landscape.	PRIORITY E	Identify, document, and articulate the evolving SLTT physical and cyber critical infrastructure threats, risks, and risk management strategies.
	PRIORITY F	Identify, document, and articulate—including providing information to DHS on—SLTT critical infrastructure program priorities, activities, best practices, capability gaps, and needs.
	PRIORITY G	Share best practices and promote Federal critical infrastructure programs, tools, and capabilities to SLTT agencies to fill capability gaps and needs.
3 **ENGAGE SLTT GOVERNMENT PARTNERS ON CRITICAL INFRASTRUCTURE ISSUES** Leverage the Council's working groups, initiatives, and products to educate colleagues in other jurisdictions on critical infrastructure issues.	PRIORITY H	Facilitate NIPP 2013 awareness and implementation with SLTT governments.
	PRIORITY I	Facilitate networking between SLTT agencies and personnel to obtain their viewpoints on and communicate best practices in critical infrastructure security and resilience.
4 **COLLABORATE WITH THE CRITICAL INFRASTRUCTURE COMMUNITY** Work with DHS, other DHS partnership councils, the critical infrastructure sectors, and other critical infrastructure partners on projects of common interest.	PRIORITY J	Conduct joint initiatives with other DHS partnership councils to support efforts to plan, implement, and execute the Nation's critical infrastructure security and resilience mission.
	PRIORITY K	Provide senior-level, cross-jurisdictional strategic communications and coordination through partnership with DHS and critical infrastructure owners and operators.
	PRIORITY L	Coordinate with others focusing on the critical infrastructure mission (e.g., regional, international, academic, and research organizations) to gather best practices and lessons learned and discuss improvements to Federal programs and products.
5 **CONTRIBUTE TO NATIONAL CRITICAL INFRASTRUCTURE POLICIES AND FEDERAL PROGRAMS, TOOLS, AND CAPABILITIES** Leverage the Council's working groups to collaborate with DHS to ensure Federal critical infrastructure policies, plans, programs, tools, and capabilities meet SLTT government needs.	PRIORITY M	Contribute to the development of new or updated national-level documents guiding critical infrastructure policy.
	PRIORITY N	Work with DHS to coordinate issue resolution and provide the SLTT perspective on enhancing Federal critical infrastructure programs, tools, and capabilities to ensure effectiveness in the field.

4.2 SLTTGCC Activities

The SLTTGCC developed a set of 26 concrete activities that provide the framework to implement the Council's vision and mission to integrate the SLTT perspective in Federal critical infrastructure plans and programs and to facilitate collaboration across jurisdictions. Table 2 presents these collaborative, voluntary activities that the Council intends to pursue over the next 1–4 years. The activities focus on ensuring the Council remains a robust organization that consistently provides value to the critical infrastructure community, leveraging a number of high-priority Federal critical infrastructure programs, and collaborating with specific organizations on issues of common interest.

While the SSPs are updated every four years, the Council will annually prioritize and develop a list of discrete, detailed activities to pursue over the coming year, considering timing, available resources, and feasibility. During this time, the Council may also update the activities to reflect evolving risk, additional requests from Federal agencies to provide the SLTT perspective, progress, or completion.

Table 2. SLTTGCC Priorities and Activities

Map to Priority	SLTTGCC Activities	
Ⓐ	1	Grow the Council to one member per State with a balance between levels of government and disciplines by identifying and recruiting candidates from key geographical and discipline areas not currently represented.
Ⓐ	2	Develop a new-member welcome packet inclusive of information helpful to critical infrastructure personnel, such as Council and Protective Security Advisor contact information, Federal critical infrastructure program list, and NIPP 2013 summary.
ⒷⒸ	3	Annually review the Council's subject matter expert and Alliance Network lists to ensure appropriate personnel are listed; recruit, add, and delete as necessary.
Ⓓ	4	Annually review the Sector Liaison roster to ensure each sector is assigned one primary and one alternate liaison and distribute liaison positions across the full membership; finalize a process for reporting meeting attendance.
Ⓔ	5	Examine the changing critical infrastructure mission implementation by SLTT agencies; conduct annual targeted outreach to partners in each region to identify and highlight emerging issues, challenges, and best practices in risk management.
Ⓔ	6	Develop guidance (e.g., white papers) for SLTT agencies to enhance their understanding of, management of, and response to increased cyber threats to critical infrastructure.
Ⓔ	7	Examine the future role of credentialing for physical, logical, and disaster response; distribute to partners summaries focused on challenges, joint pilot projects, and best practices.
Ⓕ	8	Develop a dissemination process for all Council products to share with members, subject matter experts, Alliance Network, the sectors, and the DHS Office of Infrastructure Protection.
Ⓖ	9	Examine current critical infrastructure training offerings and suggest updates to topics based on the changing critical infrastructure mission.
Ⓖ	10	Facilitate the connection between Federal critical infrastructure pilot program opportunities and SLTT agencies able to serve as a test site for the program.
Ⓗ	11	Develop a summary of Federal critical infrastructure programs for use by SLTT agencies.
Ⓘ	12	Develop best practice summaries and guides (e.g., Administrator, User) for SLTT agency use when implementing IP Gateway.
Ⓘ	13	Host at least six virtual engagements (e.g., Real-Time Forum Webinars) each year to facilitate a discussion between SLTT critical infrastructure professionals on issues, challenges, programs, and best practices.

Map to Priority	SLTTGCC Activities	
J	14	Conduct regular joint meetings/calls with partnership councils (e.g., Cross-Sector Coordinating Council, Federal Senior Leadership Council, RC3 Executive Committee, Partnership for Critical Infrastructure Security, and the National Infrastructure Advisory Council) on issues of common interest.
K	15	Assist the critical infrastructure sectors implementing Sector-Specific Plan activities focused on engagement with SLTT governments and agencies.
K	16	Partner with DHS and InfraGard to host Joint Critical Infrastructure Partnership Webinars (at least quarterly) to engage partners nationwide on critical infrastructure issues.
K	17	Participate in DHS-sponsored classified and unclassified threat and incident calls to convey the SLTT perspective and aid in the dissemination of information to SLTT agencies.
K	18	Facilitate regular interaction between the Council, the Regional Directors, and Protective Security Advisors, including holding joint meetings/sessions on issues of common interest (e.g., regionalization and assessments).
L	19	Facilitate regular interaction between the Council and the National Council of ISACs to share best practices and lessons learned on issues of common interest.
M	20	Serve on working groups led by DHS and/or submit comments on national-level documents, including presidential policy directives, national plans and frameworks, and sector plans.
N	21	Work with the DHS Office of Infrastructure Protection (IP) on IP Gateway requirements development process, future use of the tool, and assessment training.
N	22	Work with DHS to improve the robustness and ease of use of the HSIN-SLTTGCC platform.
N	23	Work with FEMA on the critical infrastructure components of the Threat and Hazard Identification and Risk Assessment (THIRA) and State Preparedness Report.
N	24	Work with the DHS National Protection and Programs Directorate (NPPD) to enhance cyber capabilities and resources provided by the Protective Security Advisors and Cyber Security Advisors to SLTT critical infrastructure programs and fusion centers.
N	25	Work with the DHS Office for Bombing Prevention (OBP) to enhance the efficacy and availability of counter-improvised explosive device (IED) training and awareness courses.
N	26	Work with DHS Science and Technology Directorate and the Technology Transfer Working Group on credentialing.

SLTTGCC Contributions to Sector Activities

The 2015 SSPs include goals and priorities to guide each sector's security and resilience efforts over the next four years, as well as activities that sector partners (e.g., SCCs and GCCs) plan to collaboratively conduct to improve the security and resilience of the sector. Many activities included in the SSPs identify the need to specifically engage with SLTT governments or agencies. The SLTTGCC, as included in Activity 15, can provide access to members and subject matter experts to facilitate collaboration between the sectors and the SLTT critical infrastructure community. In addition, regular interaction between Council members and the sectors in their jurisdictions and regions can aid the implementation of these activities and the building of regional security and resilience capacity. As described in further detail in each SSP, SLTT-focused activities include:

- **Information Sharing:** Facilitate the sharing of information between levels of government (including fusion centers) and the critical infrastructure sectors.
- **Stakeholder Engagement:** Collaborate on cross-jurisdictional issues, such as information sharing, exercises, and emergency response.
- **Strategic Planning and Coordination:** Evaluate and develop strategies on emerging issues.
- **Education, Training, and Exercises:** Identify SLTT resources and personnel to support training and exercises.

- **Technical Assistance and Best Practices:** Increase partner awareness and use of Federal critical infrastructure tools and programs and identify and document best practices (e.g., communication, risk management, and cybersecurity).
- **Incident Management:** Develop capabilities to assess asset functionality and share resources during an incident, and collaborate on crisis reentry, access control, and credentialing issues.

4.3 Measuring Effectiveness of Activities

Performance measurement efforts are an important step in determining the effectiveness of risk management investments, programs, and activities. Where possible, the Council attempts to measure how its voluntary partnership activities contribute to risk reduction and enhanced resilience across the SLTT landscape without precluding or impinging the measurement efforts of individual SLTT partners. An established performance metrics system designed by DHS to track the progress of Council activities is used to ensure accurate and consistent measurement.

Table 3 aligns SLTTGCC activities with a set of possible performance metrics that may be used to measure and report progress, where possible. The metrics not only measure the completion of the activity—using output measures such as the number of products developed or partners engaged—but also aim to measure the outcomes of these activities—particularly how effective they are in achieving progress toward Council goals. The list is not exhaustive of all possible ways to measure effectiveness. The Council may voluntarily measure and report additional information on its progress in future reporting efforts.

Table 3. Expected Metrics for SLTTGCC Activities

	SLTTGCC Activities	Expected Metrics
1	Grow the Council to one member per State with a balance between levels of government and disciplines by identifying and recruiting candidates from key geographical and discipline areas not currently represented.	• Number of Council members and government affiliation per State • Number of potential candidates identified and members added • Key geographical and discipline areas for development
2	Develop a new-member welcome packet inclusive of information helpful to critical infrastructure personnel, such as Council and Protective Security Advisor contact information, Federal critical infrastructure program list, and NIPP 2013 summary.	• Status of new-member packed development • Products developed and their distribution
3	Annually review the Council's subject matter expert and Alliance Network lists to ensure appropriate personnel are listed; recruit, add, and delete as necessary.	• Status of subject matter expert and Alliance Network lists reviews • Number of subject matter experts and Alliance Network members recruited or added • Products developed and their distribution
4	Annually review the Sector Liaison roster to ensure each sector is assigned one primary and one alternate liaison and distribute liaison positions across the full membership; finalize a process for reporting meeting attendance.	• Status of Sector Liaison roster review • Status of membership liaison distribution • Products developed and their distribution • Status of liaison meeting attendance process finalization

	SLTTGCC Activities	Expected Metrics
5	Examine the changing critical infrastructure mission implementation by SLTT agencies; conduct annual targeted outreach to partners in each region to identify and highlight emerging issues, challenges, and best practices in risk management.	• Number of meetings and workshops organized or coordinated with SLTT partners to capture mission challenges and best practices and level of participation over time • Challenges and best practices identified • Products developed and their distribution • How participants and recipients intend to use the information provided
6	Develop guidance (e.g., white papers) for SLTT agencies to enhance their understanding of, management of, and response to increased cyber threats to critical infrastructure.	• Status of guidance development • Number of meetings and workshops organized or coordinated with SLTT partners to promote cybersecurity awareness and cyber threat management • Products developed and their distribution • How participants and recipients intend to use the information provided
7	Examine the future role of credentialing for physical, logical, and disaster response; distribute to partners summaries focused on challenges, joint pilot projects, and best practices.	• Number of meetings and workshops organized or coordinated with SLTT partners to capture credentialing challenges and best practices and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
8	Develop a dissemination process for all Council products to share with members, SMEs, Alliance Network, the sectors, and IP.	• Status of dissemination process development per target group
9	Examine current critical infrastructure training offerings and suggest updates to topics based on the changing critical infrastructure mission.	• Status of training examination and suggested updates • Products developed and their distribution • How participants and recipients intend to use the information provided
10	Facilitate the connection between Federal critical infrastructure pilot program opportunities and SLTT agencies able to serve as a test site for the program.	• Number of meetings and workshops organized or coordinated with DHS and SLTT partners to identify Federal critical infrastructure pilot program opportunities • Pilot programs and SLTT agencies selected
11	Develop a summary of Federal critical infrastructure programs for use by SLTT agencies.	• Status of summary of Federal critical infrastructure programs • Products developed and their distribution • How participants and recipients intend to use the information provided

	SLTTGCC Activities	Expected Metrics
12	Develop best practice summaries and guides (e.g., Administrator, User) for SLTT agency use when implementing IP Gateway.	• Number of meetings and workshops organized or coordinated with SLTT partners to capture IP Gateway implementation best practices • Status of best practice summaries and guides development • Products developed and their distribution • How participants and recipients intend to use the information provided
13	Host at least six virtual engagements (e.g., Real-Time Forum Webinars) each year to facilitate a discussion between SLTT critical infrastructure professionals on issues, challenges, programs, and best practices.	• Number of virtual engagements hosted and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
14	Conduct regular joint meetings/calls with partnership councils (e.g., Cross-Sector Coordinating Council, RC3 Executive Committee, Partnership for Critical Infrastructure Security, and the National Infrastructure Advisory Council) on issues of common interest.	• Number of meetings or calls organized or coordinated with the Cross-Sector Coordinating Council, Federal Senior Leadership Council, RC3Executive Committee, Partnership for Critical Infrastructure Security, and the National Infrastructure Advisory Council and level of participation over time
15	Assist the critical infrastructure sectors implementing Sector-Specific Plan activities focused on engagement with SLTT governments and agencies.	• Number of meetings and workshops organized or coordinated with sector partners to assist with SLTT engagement
16	Partner with DHS and InfraGard to host Joint Critical Infrastructure Partnership Webinars (at least quarterly) to engage partners nationwide on critical infrastructure issues.	• Number of Joint Critical Infrastructure Partnership Webinars hosted and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
17	Participate in DHS-sponsored classified and unclassified threat and incident calls to convey the SLTT perspective and aid in the dissemination of information to SLTT agencies.	• Number of DHS-sponsored threat and incident calls to which the Council contributed and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
18	Facilitate regular interaction between the Council, the Regional Directors, and Protective Security Advisors, including holding joint meetings/sessions on issues of common interest (e.g., regionalization, assessments).	• Number of meetings and workshops organized or coordinated with Regional Directors and Protective Security Advisors on SLTT-relevant critical infrastructure security and resilience issues • Products developed and their distribution • How participants and recipients intend to use the information provided

	SLTTGCC Activities	Expected Metrics
19	Facilitate regular interaction between the Council and the National Council of ISACs to share best practices and lessons learned on issues of common interest.	• Number of meetings or calls organized or coordinated with the National Council of ISACs and level of participation over time • Products developed and their distribution • How participants and recipients intend to use the information provided
20	Serve on working groups led by DHS and/or submit comments on national-level documents, including presidential policy directives, national plans and frameworks, and sector plans.	• Number of meetings or calls organized or coordinated with DHS on national-level documents • National-level documents to which the Council provided input
21	Work with DHS IP on IP Gateway requirements development process, future use of the tool, and assessment training.	• Number of meetings and workshops organized or coordinated with DHS on IP Gateway • Status of engagement on requirements development, future use, and training • Products developed and their distribution • How participants and recipients intend to use the information provided
22	Work with DHS to improve the robustness and ease of use of the HSIN-SLTTGCC platform.	• Number of meetings and workshops organized or coordinated with DHS on HSIN-SLTTGCC enhancements • Status of improvements
23	Work with FEMA on the critical infrastructure components of the THIRA and State Preparedness Report.	• Number of meetings and workshops organized or coordinated with FEMA on THIRA and State Preparedness Report critical infrastructure components • Products developed and their distribution • How participants and recipients intend to use the information provided
24	Work with DHS NPPD to enhance cyber capabilities and resources provided by the Protective Security Advisors and Cyber Security Advisors to SLTT critical infrastructure programs and fusion centers.	• Number of meetings and workshops organized or coordinated with DHS NPPD on cyber capability and resource enhancements for SLTT programs and fusion centers • Products developed and their distribution • How participants and recipients intend to use the information provided
25	Work with DHS OBP to enhance the efficacy and availability of counter-IED training and awareness courses.	• Number of meetings and workshops organized or coordinated with DHS OBP on counter-IED training and awareness courses • Number of courses provided to SLTT partners • Products developed and their distribution • How participants and recipients intend to use the information provided
26	Work with the DHS Science and Technology Directorate and the Technology Transfer Working Group on credentialing.	• Number of meetings and workshops organized or coordinated with DHS Science and Technology Directorate on credentialing • Products developed and their distribution • How participants and recipients intend to use the information provided

APPENDIX A. ACRONYMS AND TERMS

ACAMS	Automated Critical Asset Management System
DHS	U.S. Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GCC	Government Coordinating Council
GIS	Geospatial Information System
HIRA	Hazard Identification and Risk Assessment
HSIN	Homeland Security Information Network
I&A	DHS Office of Intelligence and Analysis
IED	Improvised Explosive Device
IP	DHS Office of Infrastructure Protection
ISAC	Information Sharing and Analysis Center
JCIP	Joint Critical Infrastructure Partnership
LEPC	Local Emergency Planning Committee
NCIPP	National Critical Infrastructure Protection Program
NPPD	National Protection and Programs Directorate
NIPP 2013	National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience
OBP	DHS Office for Bombing Prevention
PSA	Protective Security Advisor
RC3	Regional Consortium Coordinating Council
RD	Regional Director
RRAP	Regional Resiliency Assessment Program
SCC	Sector Coordinating Council
SLTT	State, local, tribal, and territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SME	Subject Matter Expert
SSP	Sector-Specific Plan
THIRA	Threat and Hazard Identification and Risk Assessment
TRIPwire	Technical Resource for Incident Prevention
UASI	Urban Areas Security Initiative

APPENDIX B. SLTTGCC ACTIVITIES: ALIGNMENT WITH THE NIPP 2013 (CHART)

Table B1. SLTTGCC Priorities Aligned with Joint National Priorities and NIPP 2013 Goals

SLTTGCC Priorities		Joint National Priorities					NIPP 2013 Goals				
		Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	1	2	3	4	5
A	Identify, recruit, and maintain membership			PRIORITY A						X	
B	Identify, recruit, and maintain subject matter experts			PRIORITY B						X	
C	Identify, recruit, and maintain Alliance Network			PRIORITY C						X	
D	Maintain Sector Liaison program			PRIORITY D						X	
E	Identify SLTT threats, risks, and risk management strategies	PRIORITY E					X				
F	Identify SLTT priorities, activities, best practices, capability gaps, and needs		PRIORITY F				X				
G	Share best practices and promote Federal programs, tools, and capabilities	PRIORITY G	PRIORITY G	PRIORITY G	PRIORITY G	PRIORITY G				X	X
H	Facilitate NIPP 2013 awareness and implementation					PRIORITY H				X	
I	Facilitate networking between SLTT agencies and personnel			PRIORITY I	PRIORITY I	PRIORITY I				X	X
J	Conduct joint initiatives with other DHS partnership councils		PRIORITY J	PRIORITY J	PRIORITY J				X	X	
K	Provide strategic communications and coordination through partnership			PRIORITY K	PRIORITY K				X	X	
L	Coordinate with others focusing on the critical infrastructure mission			PRIORITY L	PRIORITY L				X	X	
M	Contribute to the development of new or updated national-level documents				PRIORITY M					X	
N	Work with DHS on enhancing Federal programs, tools, and capabilities		PRIORITY N	PRIORITY N	PRIORITY N			X			

NIPP 2013 Goals

1. Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
2. Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.
3. Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services.
4. Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
5. Promote learning and adaptation during and after exercises and incidents.

Table B2. Contribution of the SLTTGCC Activities to the NIPP 2013 Calls to Action

SLTTGCC Contribution or Aligned Activity		NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
1	Grow the Council to one member per State with a balance between levels of government and disciplines by identifying and recruiting candidates from key geographical and discipline areas not currently represented.			X									
2	Develop a new-member welcome packet inclusive of information helpful to critical infrastructure personnel, such as Council and Protective Security Advisor contact information, Federal critical infrastructure program list, and NIPP 2013 summary.									X			
3	Annually review the Council's subject matter expert and Alliance Network lists to ensure appropriate personnel are listed; recruit, add, and delete as necessary.			X								X	
4	Annually review the Sector Liaison roster to ensure each sector is assigned one primary and one alternate liaison and distribute liaison positions across the full membership; finalize a process for reporting meeting attendance.			X								X	
5	Examine the changing critical infrastructure mission implementation by SLTT agencies; conduct annual targeted outreach to partners in each region to identify and highlight emerging issues, challenges, and best practices.		X										
6	Develop guidance (e.g., white papers) for SLTT agencies to enhance their understanding of, management of, and response to increased cyber threats to critical infrastructure.									X			
7	Examine the future role of credentialing for physical, logical, and disaster response; distribute to partners summaries focused on challenges, joint pilot projects, and best practices.									X			
8	Develop a dissemination process for all Council products to share with members, SMEs, Alliance Network, the sectors, and IP.					X							
9	Examine current critical infrastructure training offerings and suggest updates to topics based on the changing critical infrastructure mission.									X			
10	Facilitate the connection between Federal critical infrastructure pilot program opportunities and SLTT agencies able to serve as a test site for the program.				X					X	X		
11	Develop a summary of Federal critical infrastructure programs for use by SLTT agencies.									X			
12	Develop best practice summaries and guides (e.g., Administrator, User) for SLTT agency use when implementing IP Gateway.									X			

	SLTTGCC Contribution or Aligned Activity	NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
13	Host at least six virtual engagements (e.g., Real-Time Forum Webinars) each year to facilitate a discussion between SLTT critical infrastructure professionals on issues, challenges, programs, and best practices.									X			
14	Conduct regular joint meetings/calls with partnership councils (e.g., Cross-Sector Coordinating Council, RC3 Executive Committee, Partnership for Critical Infrastructure Security, and the National Infrastructure Advisory Council) on issues of common interest.		X										
15	Assist the critical infrastructure sectors implementing Sector-Specific Plan activities focused on engagement with SLTT governments and agencies.		X										
16	Partner with DHS and FBI InfraGard to host Joint Critical Infrastructure Partnership Webinars (at least quarterly) to engage partners nationwide on critical infrastructure issues.									X			
17	Participate in DHS-sponsored classified and unclassified threat and incident calls to convey the SLTT perspective and aid in the dissemination of information to SLTT agencies.		X			X							
18	Facilitate regular interaction between the Council, the Regional Directors, and Protective Security Advisors, including holding joint meetings/sessions on issues of common interest (e.g., regionalization, assessments).		X							X			
19	Facilitate regular interaction between the Council and the National Council of ISACs to share best practices and lessons learned on issues of common interest.									X	X		
20	Serve on working groups led by DHS and/or submit comments on national-level documents, including presidential policy directives, national plans and frameworks, and sector plans.	X	X										
21	Work with DHS IP on IP Gateway requirements development process, future use of the tool, and assessment training.									X	X		
22	Work with DHS to improve the robustness and ease of use of the HSIN-SLTTGCC platform.					X				X	X		
23	Work with FEMA on the critical infrastructure components of the Threat and Hazard Identification and Risk Assessment (THIRA) and Preparedness Report.									X	X		
24	Work with DHS NPPD to enhance cyber capabilities and resources provided by the Protective Security Advisors and Cyber Security Advisors to SLTT critical infrastructure programs and fusion centers.					X				X			
25	Work with the DHS OBP to enhance the efficacy and availability of counter-IED training and awareness courses.									X			
26	Work with DHS Science and Technology Directorate and the Technology Transfer Working Group on credentialing.									X			
	SLTTGCC goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1.	X											
	Development of the 2015 SLTTGCC Annex meets Call to Action #2.		X										
	The SLTTGCC supports Call to Action #10 by working with its Federal partners to implement the National Critical Infrastructure Security and Resilience Research and Development Strategy.										X		
	The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the SLTTGCC to evaluate and report on the progress of partnership efforts in support of Call to Action #11.											X	

NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

Call to Action #4: Leverage Incentives to Advance Security and Resilience

Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Call to Action #11: Evaluate Progress Toward the Achievement of Goals

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

Homeland
Security