5N5 | Information Guide

WHAT IS 5N5?

5N5 is a cybersecurity workshop series on/about "*five non-technical actions to consider in five days*". It is specifically designed for transportation owners and operators to learn about Department of Homeland Security resources and programs available to them, as well as non-technical policy or procedural actions that can be implemented to enhance their company or agency's cybersecurity posture.

WHAT IS THE AUDIENCE FOR 5N5?

5N5 is designed for policy and security professionals responsible for their organization's risk management, emergency preparedness and security practices, not just for those in charge of IT security.

WHAT IS THE PURPOSE OF 5N5?

5N5 brings together owners and operators from the different modes of transportation to facilitate the sharing of best practices and lessons learned from colleagues across the transportation sector and to cultivate those best practices and lessons learned into actionable steps to improve their security and emergency preparedness plans, training and exercise programs.

WHAT ARE THE WORKSHOP BENEFITS?

As a result of attending the 5N5 workshop series, participants will:

1. Familiarize themselves with Department of Homeland Security no cost cybersecurity resources and support programs.
2. Be able to implement cybersecurity measures based on peer-to-peer discussions of best practices and lessons learned.
3. Understand at least five non-technical actions to consider implementing in five days to enhance their agency or company's cybersecurity posture.
4. Network across the different agencies, fostering a community security operating environment
5. Understand the importance of reporting cyber intrusion incidents

WHAT IS THE STRUCTURE OF 5N5?

The one-day workshop is designed to assist participants with understanding the NIST Framework and may discover possible security gaps within their organization, and demonstrate ways to incorporate actionable measures into security planning. This workshop includes facilitated dialogue and small group work sessions and activities.

Transportation Security Administration

HOST RESPONSIBILITIES

The workshop host is in charge of: 1) providing a suitable venue; 2) assembling an appropriate planning team; and 3) ensuring the correct people from their enterprise attend the workshop.

Prior to the workshop, TSA conducts multiple planning conference calls with the host and the planning team. The goal of these meetings is to complete administrative requirements and answer any logistical workshop questions or concerns.

TSA RESPONSIBILITIES

Transportation Security Inspectors (TSIs) are responsible for drafting the invitation list to include multi modal participants and sending out the save-the-date. TSIs attend all planning call meetings and provide dry run and day-of help, including setup and workshop evaluations.

Regional Security Inspectors (RSIs) are responsible for making sure there is proper coordination and communication with TSA senior leadership in the local field office, including working with the Federal Security Director's front office to request a speaking engagement at the event. RSIs provide assistance to the TSIs in the event they need help developing the invite roster. They are encouraged to review the Quick Look and After Action Brief for content errors prior to publishing the final draft. RSIs are encouraged to provide the program lead a list of prioritized locations (three to five) for the 5N5 training sessions so that HQ can create fiscal year work plans for the workshops.

TSA Headquarters (HQ) is responsible for coordinating the workshop, including planning meetings, agendas and meeting notes, and logistics. HQ is responsible for ensuring all workshop materials arrive at the destination on time. HQ is responsible for working with Cyber and Infrastructure Security Agency to secure the Cybersecurity Advisors for workshop delivery. HQ provides input and coordination concerning peer-to-peer speakers as well as the guidance on the threat briefing, day-of workshop agenda, assists in drafting the invitation list to include multi-modal participants, tracks participant responses, and provides evaluators. HQ composes the Quick Look and After Action Brief.

ROLE OF THE PLANNING TEAM

The planning team assists the host in completing all requirements for the workshop. The planning team provides input and coordination concerning speakers, assists in drafting the invitation list to include multi-modal participants, and generally champions the workshop within(for) their agency. Successful planning teams have representation from different disciplines within their organization.

RECOMMENDED LIST OF PARTICIPANTS

This workshop targets policy and security professionals in multi-modes of transportation that include, but are not limited to:

- ✓ **IT Professionals:** cyber experts, IT specialists, IT managers
- ✓ **Law Enforcement:** dedicated police force, special agents, special operations, joint terrorism task force, regional working groups, fusion center/intelligences, investigation
- ✓ **Management:** CEO, President, Vice Presidents, Directors
- ✓ **Security Professionals**: Security managers, risk managers, training managers
- ✓ **Front-line Employees:** personnel, supervisors, system operators, dispatch
- ✓ **Intelligence:** Fusion centers, intelligence analysts, field intelligence officers
- ✓ **Plans and Policy:** cyber, physical, risk, employees, supervisors
- ✓ **Government Partners:** Federal, state, and local

TSA recommends limiting attendance to 35 to 50 participants but have accommodated 80-100. Participants should be available for the duration of the workshop.

5N5 | Host Planning Guide

WHAT IS 5N5?

5N5 is a cybersecurity workshop series on/about "*five non-technical actions to consider in five days*". It is specifically designed for transportation owners and operators to learn about Department of Homeland Security resources and programs available to them, as well as non-technical policy or procedural actions that can be implemented to enhance their company or agency's cybersecurity posture.

WHO IS THE AUDIENCE FOR 5N5?

5N5 is designed for policy and security professionals responsible for their organization's risk management, emergency preparedness and security practices, not just for those in charge of IT security.

WHAT IS THE PURPOSE OF 5N5?

5N5 brings together owners and operators from the different modes of transportation to facilitate the sharing of best practices and lessons learned from colleagues across the transportation sector and to cultivate those best practices and lessons learned into actionable steps to improve their security and emergency preparedness plans, training and exercise programs.

WHAT ARE THE WORKSHOP BENEFITS?

As a result of attending the 5N5 workshop series, participants will:

1. Know where to go for Department of Homeland Security cybersecurity resources and support programs.
2. Be able to implement cybersecurity measures based on peer-to-peer discussions of best practices and lessons learned.
3. Understand at least five non-technical actions to consider implementing in five days to enhance their agency or company's cybersecurity posture.
4. Network across the different agencies, fostering a community security operating environment
5. Understand the importance of reporting cyber intrusion incidents

WHAT IS THE STRUCTURE OF 5N5?

The one-day workshop is designed to assist participants with understanding the NIST Framework and may discover possible security gaps within their organization, and demonstrate ways to incorporate actionable measures into security planning. This workshop includes facilitated dialogue and small group work sessions and activities.

HOST RESPONSIBILITIES

The workshop host is in charge of: 1) providing a suitable venue; 2) assembling an appropriate planning team; and 3) ensuring the correct people from their enterprise attend the workshop.

Prior to the workshop, TSA conducts multiple planning conference calls with the host and the planning team. The goal of these meetings is to complete administrative requirements and answer any logistical workshop questions or concerns.

ROLE OF THE PLANNING TEAM

The planning team assists the host in completing all requirements for the workshop. The planning team provides input and coordination concerning speakers, assists in drafting the invitation list to include multi-modal participants, and generally champions the workshop within(for) their agency. Successful planning teams have representation from different disciplines within their organization. TSA Headquarters completes the Quick Look and After Action Brief.

RECOMMENDED LIST OF PARTICIPANTS

This workshop targets policy and security professionals in multi-modes of transportation that include, but are not limited to:

- ✓ **IT Professionals:** cyber experts, IT specialists, IT managers
- ✓ **Law Enforcement:** dedicated police force, special agents, special operations, joint terrorism task force, regional working groups, fusion center/intelligences, investigation
- ✓ **Management:** CEO, President, Vice Presidents, Directors
- ✓ **Security Professionals**: Security managers, risk managers, training managers
- ✓ **Front-line Employees:** personnel, supervisors, system operators, dispatch
- ✓ **Intelligence:** Fusion centers, intelligence analysts, field intelligence officers
- ✓ **Plans and Policy:** cyber, physical, risk, employees, supervisors
- ✓ **Government Partners:** Federal, state, and local

TSA recommends limiting attendance to between 35 and 70 participants. Participants should be available for the duration of the workshop.

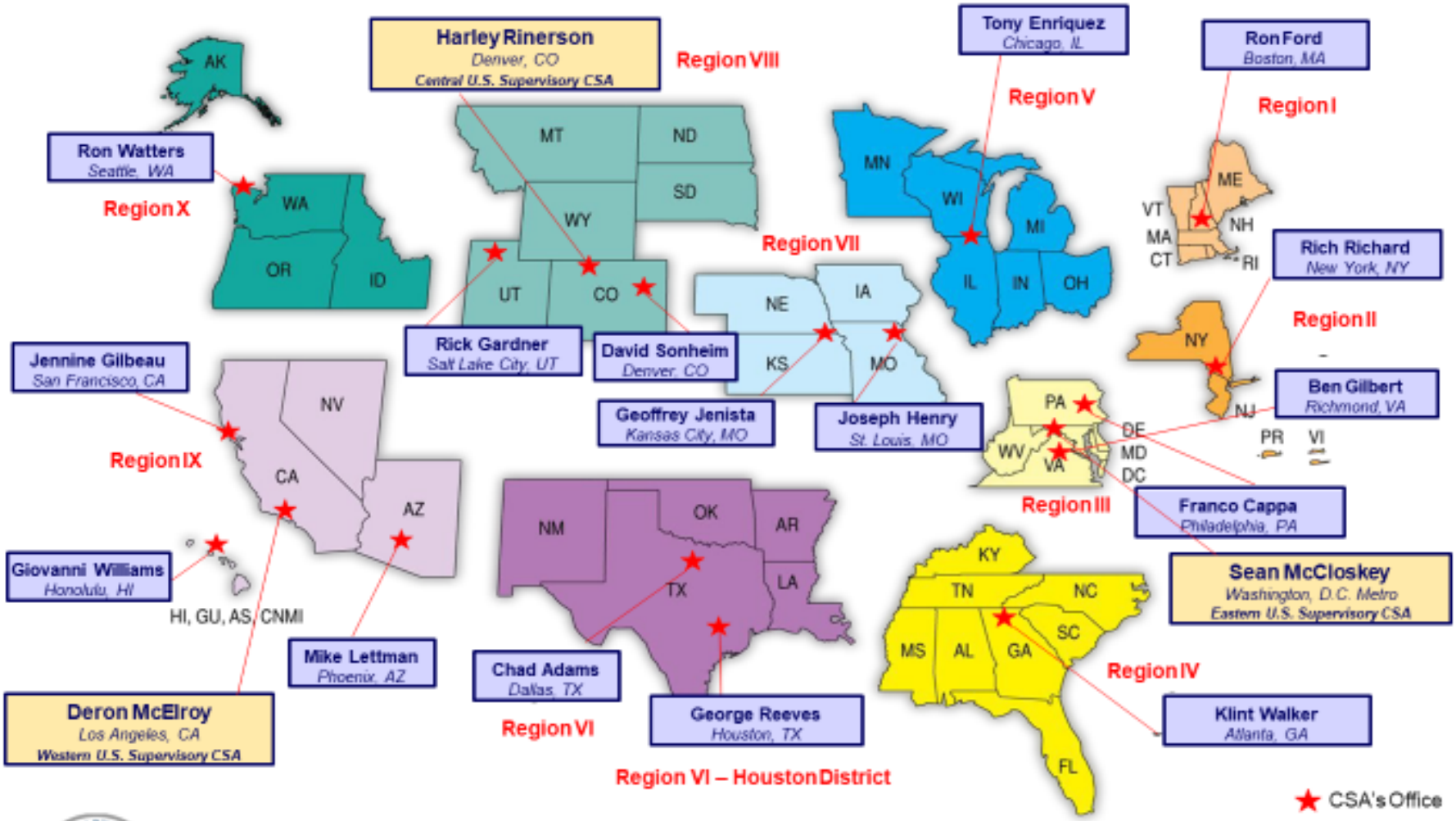
Venue Checklist

The host should provide TSA with a venue that meets the following requirements:

- 1 plenary room (holds all participants and federal team); preferred set-up: pods (6-8 people per pod) with one table for note takers (access to outlets)
- IT: audio/visual (i.e. projectors, screens, sound system) access to Internet, lapel microphones, handheld microphones
- Parking: sufficient for participants or local parking area close to the venue
- Meals/Breaks
- Secure Storage: locked space for workshop materials – can the team set up the day before?
- Other: registration area/table for sign-in and badges

The venue should be available for set-up the afternoon prior to the workshop and open to the team by no later than 7AM.

CSA Deployed Personnel



Homeland Security