

# Chapter 7

## Security Support

---

### OVERVIEW

Developing a comprehensive security plan is critical to the successful receipt, distribution, and dispensing of SNS assets during an emergency. A large public health emergency will likely produce many casualties and it will also produce concern, fear, and maybe panic within the affected community. The arrival of SNS assets will be newsworthy and may make SNS operations a magnet for persons unwilling to wait for the planned dispensing of drugs or other medical assets to protect or treat them and their families. During a deliberate attack, your SNS response organization may become a target of terrorists or terrified citizens. A detailed security plan that describes the steps required to protect

- SNS assets,
- the various locations used to support an SNS response,
- the people that support SNS response operations, and
- the SNS transportation infrastructure that supports SNS operations

is an essential component of your overall SNS preparedness planning.

We recommend enlisting the support of law-enforcement and security experts to develop your security plan. Additionally, establishing a security-support team leader to manage the security staff, resources available, and missions required to support SNS response activities is an essential component of your security plan.

In this chapter, we will explain the various security missions to consider when developing plans to protect the major functions of an SNS response. The SNS response has three critical functions that require detailed security planning and the establishment of detailed security measures:

- receiving SNS assets,
- distributing SNS assets, and
- dispensing SNS assets.



---

Each of these functions presents its own unique security challenges; but all of them require protecting critical locations, medical assets, people, and equipment.

Topics covered in this chapter include:

- security missions and tasks
- forming security-support teams
- collaboration and preparation
- mobilizing your security-support team
- badging and credentialing
- risk assessment
- POD-specific risk assessment
- security prior to the transfer of SNS assets
- security following transfer
- RSS warehouse protection
- distribution-system protection
- SNS protection in a natural or technological disaster

## SECURITY MISSIONS AND TASKS:

Developing security plans for an SNS deployment is one of the most complex functions in an SNS response. It is a resource-intensive function that requires detailed planning and coordination with numerous agencies at various levels of government as well as within the local community. It rivals the dispensing function for the number of staff needed for successful implementation. We have identified three categories of security missions that you will have to plan for during an SNS response and that are equally applicable to receiving, distributing and dispensing SNS assets.

- **Physical Security:** Establishing measures to prevent or deter access to a site or facility, resource, or information stored on physical media.
- **Personnel Protection:** Establishing security measures to ensure the safeguarding of staff involved in SNS operations and citizens receiving SNS assets.
- **Law Enforcement:** Apprehending and/or arresting those in violation of the law who may attempt to disrupt the SNS operations.

We have identified nine security missions to consider planning for during an SNS response:

- 
- Securing the airfield landing site for arriving SNS assets or, if it arrives by land, securing a meeting point where the truck convoy carrying SNS assets crosses into your state
  - Securing your RSS site(s)
  - Securing your POD(s)
  - Escorting truck convoys of SNS assets to your RSS site;
  - Escorting your distribution trucks as they negotiate traffic to make deliveries [an additional planning consideration: this task may expand because of civil unrest and may warrant personnel security measures (escorts) for drivers]
  - Controlling traffic at and around PODs
  - Coordinating parking at PODs
  - Conducting crowd control at PODs
  - Protecting staff and citizens at PODs

Depending on how you structure your overall SNS response, you also may have to plan for one or more of the following security tasks:

- Securing staging/enrollment areas if using the segmented (“spoke-and-hub”) strategy<sup>1</sup> for dispensing; during a terrorist attack, a large crowd gathered in one area could be a potential target for a secondary attack
- Escorting busses that transport the public from staging/enrollment areas to PODs [Note that using a segmented strategy may not reduce the number of security-support team members you will need to deploy at your PODs. The public will quickly learn where your PODs are located. Those who have arrived there will spread the word by cell phone as they stand in line. So, your crowd-control and staff-protection tasks remain. Also, some people may try to access your PODs by car regardless of the public information campaign that directs them not to. Traffic control and parking coordination also remain important tasks at your PODs.]
- Providing on-truck protection for U.S. Postal Service workers (if your area is offered and elects to use the Postal Plan<sup>2</sup> to assist with dispensing)

---

<sup>1</sup> We describe the segmented (“spoke and hub”) strategy in Chapter 12. Basically, it divides the POD functions of registration and dispensing. These activities would occur in different places under this strategy. The public would be asked to come first to one or more central assembly points, where they would register. They would then be bussed to a POD. After getting their drugs, they would be bussed back to their assembly point.

<sup>2</sup> The Postal Plan is based on an agreement between the U.S. Postal Service (USPS) and the departments of Homeland Security and Health and Human Services and is implemented between selected cities and the USPS. It has not been operationalized in many places. The Secretary of DHS would activate the Plan under certain circumstances if any of those places are attacked with anthrax. That attack would require treating the public very quickly to prevent disease. Under the Postal Plan, the USPS would deliver one initial 10-day drug regimen to each residential delivery address in the selected areas. This action would buy time for PODs to set up and would spread out the people coming to the PODs for more drugs. The Plan requires the city to provide each USPS delivery person with an armed law-enforcement officer for protection, requiring a large commitment of law-enforcement personnel for the 12 hours needed to carry out the Postal Plan.

- Escorting trucks moving supplies from your RSS site to secondary storage and distribution sites (if your area is using such a substructure to manage SNS assets)
- Providing security at secondary storage and distribution sites (if you have them)

Finally, we recommend you incorporate the security of existing and/or ad hoc treatment centers (hospitals, clinics) and their staff into your security plan. Depending on the type of attack, symptomatic patients may self-refer to these locations, and the crowds may become large, overwhelming the center's staff.

## FORMING YOUR SECURITY TEAM

### SNS Security Team

Under most conditions, SNS assets arrive at the state accompanied by the SNS Technical Advisory Response Unit (TARU). The United States Marshals Service (USMS), in partnership with the Centers for Disease Control and Prevention, Office of Security and Emergency Preparedness, is responsible for protecting both the TARU staff members and the deployed SNS assets until the assets are signed over (released) to the state and are no longer in federal custody. Once the assets are in state custody, the state is responsible for their effective safeguarding according to your security plan. The USMS will maintain responsibility for safeguarding the TARU and any unreleased assets until they depart the affected area. We encourage you to solicit assistance from the USMS with the Division of Strategic National Stockpile in developing your security plan.



### State Security Team

We recommend you establish a security team comprised of law-enforcement and security subject-matter experts to develop and implement your security plan. It is doubtful that one law-enforcement/security agency will be able to provide all of the resources required to support your SNS security plans. The size and specialties of your security team will, of course, depend on the number of organizations and resources available within your state. Based on the tasks required to support SNS operations, expect this team to be quite robust in size. Some law-

---

enforcement and security resources to consider adding to your security team may include:

- State police
- County sheriff
- City police
- National Guard
- University campus security
- Board of Education police
- Department of Corrections
- Department of Natural Resources/Game and Fish
- Civic organizations
- Commercial security
- Volunteers

Because this pool of resources is so large and the SNS response has many moving parts, jurisdictional boundaries and authorities will be key considerations in the development of your security plan. This is why we highly recommend using law-enforcement and security professionals to assist with developing this plan. They understand these challenges and can develop ways to overcome them and ensure a coordinated security effort.

Additionally, inherent in many of the organizations listed above are existing command structures. It may be beneficial and simpler to assign a single security task or responsibility for a single site to one law-enforcement/security agency. However you arrange it, your plans must account for security in every possible location in your area (urban, suburban, or rural) where an event may occur and SNS assets may be deployed.

## Special Considerations

The following are some coordination challenges that you may encounter as you form your security team:

- The lack of adequate manpower from a single law-enforcement agency grows as more local governments have strict budgetary constraints. Competing tasks with minimum staff to accomplish those tasks may make it difficult for an agency to support the SNS security plan.
- The sovereignty of city and county governments and the lack of elected-official buy-in can frustrate efforts to supplement a small, local law-enforcement agency. They may also prevent some law-enforcement agencies from making agreements to cover neighboring cities or counties.
- Crossing jurisdictional lines is a corollary to the sovereignty issue; here, policy or even law may limit or restrict the aid provided.

- 
- The lack of a single state-police agency makes coordinating security support more difficult than for other SNS functions. You should recruit a law-enforcement-agency matrix; that will take time, negotiating skills, and a grasp of SNS security operations.
  - No one law-enforcement agency is in charge. Although the laws of most states give great power to the public health director in an emergency, law enforcement in most states has no automatic counterpart unless directed by the governor.

### **Implement**

Establishing a strong management structure to support your security plan is extremely important. Such structure begins with selecting a security-support team leader. We recommend this person have strong law-enforcement credentials and credibility in the law-enforcement/security arena within your state. This credibility will go a long way in obtaining additional security resources through recruiting state, city, and county law-enforcement officials/security experts and their agencies to the SNS security mission. Remember, most of these agencies will have competing priorities during an emergency, possibly with already limited resources, so it is important to consider having a security leader that is (1) aware of the challenges in assembling the security support team(s); (2) knowledgeable of the security tasks required to support SNS response operations; and (3) can assist you in communicating the importance of the SNS response to the leaders of the potential resource pools, obtain their buy-in, and ultimately obtain their support. We also recommend you obtain background checks on your security-team members.

## **COLLABORATION WITH AGENCIES AND ORGANIZATIONS**

Our experience shows that it is a good practice for SNS planners and the security-support leader to discuss SNS operations and the specific security needs with law-enforcement and emergency-management planners on a continual basis. These discussions will allow both agencies to understand requirements and capabilities. As you learn their operational requirements, it will show you where to expect dedicated support to SNS security operations and where you will have resource challenges or gaps in your planning, requiring further coordination with other agencies.

Ultimately, we recommend collaboration with all agencies that may be involved in SNS operations, including federal, state and local law-enforcement/security agencies, USMS inspectors, the National Guard, the state Homeland Security Department, emergency management agencies at the state and local level, and health departments. Information exchange among these organizations will ensure effective planning and timely response.

---

## MOBILIZING YOUR SECURITY-SUPPORT TEAM

Once you have identified your security resources and developed your security team(s), an essential part of the security-support planning process is to develop the procedures necessary to get the right security team(s) to the right location(s) in a timely manner to support the SNS response operations. This is especially important for those identified as your *First-Shift* security team. Your activation and mobilization timeline will most likely be event-driven, but you can anticipate having to provide sufficient security staff to support 24/7 operations at the RSS, PODs, and other locations. Because your security team will likely come from various agencies and institutions, establishing rapid-activation procedures will be a significant challenge. But, as stated previously, your challenges can be minimized or even overcome by selecting a strong security team leader and maintaining constant dialogue with the other agencies involved as you develop your plans.

Regardless of the procedures you establish to activate and mobilize your security support team, we highly recommend the activation and mobilization process be documented in the plan, updated continually, and exercised periodically. A lack of clarity within your security-support team about which officers to call for what specific security duty (escort, RSS security, crowd control, etc) and to which shift to assign them could have a significant negative impact on SNS response operations and put many lives at risk.

## Identification Badges for Members of Your SNS Response Organization

### Implement

Most likely, your security team will be large in number and have multiple members from various agencies. Confirming the identities of all involved in your SNS response activities is extremely important to ensure the integrity of your operations. Establishing access-control measures will be a significant part of your security plan at locations. We recommend two measures for your security team to help protect your facilities and people: a comprehensive access roster that serves as an approved list of all workers expected onsite and a photo identification (ID) badge for each worker. It is best to develop your badge identification system prior to an actual event. If you must issue ID badges on the day of an event, do not conduct badging at your RSS site. This is a critical site in your SNS response infrastructure, and its location should remain confidential and as secure as possible.



We recommend that you involve the security team leader in creating an ID badge for all workers involved in SNS response. Regardless of who actually produces the badges, your security team leader should provide input

---

into the design of the badge and the data required on the badge. This precaution is necessary to ensure that, during an event, those who report to help you at the various sites are those who actually belong. Lives could depend on that assurance.

If you plan to conduct SNS operations on government, military, or private property, ID badges may be required for entry to these locations. In addition, these locations will likely raise their security levels during an event, so it is best to conduct proper coordination for entry prior to an incident as opposed to during an incident.

**Implement** We also recommend you collaborate with your health department to (1) obtain a list and (2) verify the medical credentials of health professionals expected to support your SNS operations (prior to an event, if possible).

## RISK ASSESSMENT

**Implement** We recommend the security-support team plan to conduct risk assessments at all stages of SNS response operations. They should assess the probability that adverse events/threats may follow a public health emergency or disastrous event and affect your security operations. You can then develop plans to minimize the impact of these events. The USMS assigned to protect the TARU assess *civil disturbance* as the primary threat to SNS operations. They reason that disasters create fear and that civil disturbances by fearful citizens can cause a serious threat to PODs, RSS warehouse operations, and/or your distribution network. Other adverse events include conventional crimes like theft, arson, assault, vandalism, and hijacking as well as sabotage; a secondary terrorist attack; or secondary chemical, biological, or radiological event.

A standard part of any security risk assessment is to ask and answer the following questions:

- What asset or process am I protecting?
- What potential harm or threat could occur to that asset or process?
- Who or what could be harmed and to what degree?
- Do my existing security measures help mitigate these risks?
- If not, what measures should I plan to incorporate to reduce the risks?
- Where will I accept risk in this plan?

Your detailed, written security plan should specify the answers to these questions. That way, a thorough analysis of the potential threats to your operations is conducted, and you can then establish and incorporate security measures in your plan to mitigate the threat. Once again, this will enable you to determine where there are gaps in your planning. Because of resource constraints you may not be able to incorporate measures for every potential risk. In essence, you have then accepted

---

risk in that particular area. It is recommended that those areas where you accept risk are communicated at all levels within your state hierarchy that is responsible for emergency preparedness and response. This is another area where collaboration with other agencies is key.

In conducting an SNS-related risk assessment, determine what sites, areas, assets need protection:

- Locations where SNS RSS operations will occur
- Treatment centers and PODs
- SNS support personnel, vehicles, and equipment
- SNS aircraft
- Primary and alternate routes to key facilities

As you collaborate with law enforcement to identify the potential threats against your critical SNS response locations and processes, remember to also consider the risk of potential threats in and around your RSS sites, distribution facilities, and PODs, such as

- Railways
- Petroleum pipelines
- Facilities that store or produce hazardous materials
- Facilities that may themselves become a target of terrorist attacks

## POD-SPECIFIC RISK ASSESSMENT

### Implement

Managing PODs is one of the most challenging, yet important, SNS preparedness functions, and it is vital that your security plan address how to protect not only its physical location but the people within, both staff and citizens. Providing sufficient security at PODs to help minimize unruly persons, manage chaotic flow, address traffic/parking issues, and mitigate threats to staff is essential to the overall success of your POD operations.

One challenge you may encounter is determining how strict your POD security measures should be. The mission at the POD is to ensure that the maximum number of citizens in the affected area receive prophylaxis as soon as possible; so, the intent is to process people quickly or obtain maximum throughput. There must be a balance in the security measures established to ensure safety yet not inhibit maximum throughput. Because of this fine balance in planning, we recommend the security-support team be part of the POD planning process.

The size, nature, and layout of PODs established will vary; therefore we recommend you establish a separate security operations plan for each POD, including:

- potential risk areas (e.g. large number of access points to PODs)

- 
- analysis of the surrounding area (e.g., providing adequate onsite or nearby parking near high-flow streets or freeways).
  - specific physical security measures and measures to effectively safeguard personnel at the POD
  - security measures to mitigate risk (e.g., reducing the number of access points to the POD)
  - POD layout (e.g., allowing a controlled patient flow)
  - procedures for managing disorderly persons or crowds, traffic into and out of the facility, and parking
  - traffic plans for each POD (the mix of roads, streets, and highways at each will differ)
  - number of security-support team members needed per shift per POD
  - communications resources and plans for security team members
  - security management structure (chain of command)

Whether you opt for the segmented or nonsegmented approach to managing patient flow at PODs, the level of security should remain the same. In theory, the segmented approach would minimize access to the PODs by individual vehicles, thereby reducing traffic congestion, parking etc. However, as your POD locations become known to the local community, traffic flow around the POD will likely increase and require crowd control, parking enforcement, and personnel protection.

One major difference in opting for a segmented process of patient management is that you may have to plan to secure each additional remote-staging site, conducting a risk assessment for each staging site and developing security measures to mitigate the risks identified. Additionally, you may consider providing escorts for vehicles transporting patients between the remote staging site and the POD(s).

## Security Prior to Federal Transfer of SNS Assets

As previously stated, the USMS is responsible for protecting both the TARU staff members and the SNS assets until the assets are signed over (released) to the state and no longer in federal custody.<sup>3</sup> The SNS assets will most likely arrive in your state via airplane and be transferred to trucks via trucks. The TARU will most likely arrive via airplane.

Timeliness in transporting these assets is essential, and security plans should be well developed so no delays occur in receiving the SNS.

---

<sup>3</sup> Once SNS assets are signed over to the state, the responsibility for safeguarding those assets transfers to the state. The USMS retains responsibility for safeguarding any assets that remain in federal custody and are not signed over to the state.

---

It is important to designate a member of your security team to coordinate with the USMS inspectors prior to the arrival of SNS assets. We highly recommend including such contact information in your plan to ensure coordination and collaboration. The USMS will need to have a clear understanding of your overall security plan. It will also need to know which agency is responsible for

**Implement**

- Meeting and escorting trucks moving SNS assets from the arrival airport or state line to the RSS warehouse,
- Escorting and/or transporting the TARU from the arrival airport to the RSS warehouse, and
- Safeguarding SNS aircraft at the arrival airport.

Inherent in these tasks are necessary security measures that should be planned, including traffic control on the routes and access control at the airfield.

To ensure that the USMS is adequately integrated with the law-enforcement and security operations in the affected area, we request that you provide two handheld radios connected to the local law-enforcement communication network for the duration of the operation.

## SECURITY FOLLOWING TRANSFER OF SNS ASSETS

Under normal circumstances, custody transfer of SNS assets will occur at the RSS warehouse. The critical security tasks that your plan should address upon receipt of SNS assets include

- Safeguarding the RSS warehouse;
- Safeguarding distribution vehicles while loading, offloading, and in transit; and
- Managing vehicle distribution routes.



### Safeguarding the RSS Warehouse

**Implement**

RSS warehouse protection is essential to the effective receipt of SNS assets during an event. Compromising the location of this site could impair or even halt the flow of SNS assets into your state. The best way to protect your RSS site is to ensure that security measures are in place to keep its location confidential, allowing only authorized people know its location. We recommend your security team address the following elements in protecting the RSS warehouse:

- Maintain access control at the facility.

- Require all *personnel* to enter and exit the facility through a single entrance.
- Post guards or law-enforcement officers at each entrance to the facility and establish a mechanism to check the identification of each person attempting to enter the facility. This could involve checking ID badges, sign-in logs, and visitor escorts.
- Establish multiple routes for *vehicle* entry and exit.
- Establish a perimeter of 300 to 1000 feet around the RSS warehouse within which only authorized distribution and emergency vehicles are allowed. Maintain a well-lighted facility exterior.
- Secure doors leading into or out of the facility by posting a guard at, locking, and/or alarming each door.
- Safeguard delivery and distribution trucks while they are staged and being offloaded or loaded.
- Establish crowd-control procedures that restrain or remove disorderly persons who try to disrupt RSS operations.
- Develop an evacuation plan for the facility.
- Consider the need for
  - roving patrols,
  - static guard posts,
  - roadblocks,
  - perimeter fences,
  - physical barriers of various types,
  - vehicle gates, and
  - closed-circuit television.

### Implement



## Distribution-System Protection

### Implement

The distribution system within the SNS preparedness plan will ensure that the proper medical assets are transported via trucks or other vehicles from the RSS to the PODs or treatment facilities, as required. It is imperative these vehicles have ready access to and from the RSS to ensure timely delivery. Following the terrorist attack on September 11, 2001, congestion in the National Capital Region slowed traffic to a crawl. You should anticipate similar traffic congestion during an emergency in your state. We recommend that your security plans incorporate measures to ensure unimpeded movement of your distribution vehicles throughout the affected area and that these measures are coordinated with the proper law-enforcement/security agencies. You might consider

- Coordinating law-enforcement escort of distribution vehicles to and from PODs and treatment centers;
- Securing key road networks so that only SNS and other emergency vehicles can use them; and
- Using alternative transport methods to support distribution, such as
  - Air (SNS cargo containers are designed to be sling loaded under heli-

### Deploy

- copters),
- Railroads,
- Subways, and
- Waterways.

NOTE: If alternative methods to support distribution are used to alleviate traffic congestion, you will also have to develop and coordinate your security plan to protect the transport and distribution of assets by these alternative means.

## SNS PROTECTION IN A NATURAL OR TECHNOLOGICAL DISASTER

It is important to keep in mind as you develop your security plan that SNS deployments are not strictly tied to acts of bioterrorism. The contents of the SNS are also used to support natural or technological disasters. SNS played a key role in the federal government's response to the hurricanes of 2005. There were many challenges with the use of security/law-enforcement resources during those response operations. The security resources you plan for in a bioterror emergency may not be available during a natural disaster, so it is imperative that you coordinate security resources so they can cope with all types of emergencies that may involve the deployment of SNS assets.

## PLANNING CONSIDERATIONS

Consideration	Responsibility		
	State	Regional	Local
Do you have a detailed, written plan for your security support?			
Does your plan address each security task that is applicable to your SNS response plan?			
Does your written plan incorporate law-enforcement and security agencies to provide security for the entire SNS response organization?			

Consideration	Responsibility		
	State	Regional	Local
Is your written plan based on risk assessments (at least of your PODs and your RSS) conducted by law-enforcement personnel?			
Does your plan include a call-down process for rapidly mobilizing an adequate first shift of law-enforcement/security officers to allow your security-support team to perform all of its tasks at all SNS operational locations?			
Do your written POD and RSS security plans include the base number of law-enforcement/security officers needed, post assignments, screening procedures, communications, traffic control, and crowd control?			

## Implementation Capabilities

Capability	Responsibility		
	State	Regional	Local
Have you briefed law-enforcement and emergency-management planners on the nature of SNS operations and its security requirements?			
Is your security-support team led by a law-enforcement/security expert?			
Have you assessed the risks that could interfere with SNS operations?			
Have you obtained commitments from a sufficient number of law-enforcement and security agencies to ensure that you will have security-support personnel available?			

Capability	Responsibility		
	State	Regional	Local
Have you contacted community agencies and organizations for persons to augment security by performing low-risk tasks?			
Has the law-enforcement agency responsible for the security of each POD site or RSS warehouse conducted its own risk assessment of the facility to determine if the planned number of officers and procedures for screening, traffic control, and crowd control are adequate?			
Have you tested your mobilization process?			
Has a basic background check been conducted on all state SNS volunteers?			
Do you have a written "access list" of approved state SNS volunteers/workers that can rapidly be provided to your security-support team personnel?			
Have you prepared and distributed ID badges to your screened and approved state SNS volunteers/workers?			
Do you have a rapid process for issuing ID badges to your "just-in-time" volunteers (including security-support law-enforcement officers and other personnel), TARU members, and any persons coming to help from out of your area?			
Has your public health agency checked the credentials of medical professionals involved in an SNS response?			
Have you arranged protective services for the SNS aircraft, trucks that move SNS assets to the RSS site, and vehicles transporting TARU team members?			

Capability	Responsibility		
	State	Regional	Local
Has the security team determined how it will handle disorderly persons or civil disorder at the PODs or the RSS?			
Has the security-support team determined how they will communicate with and coordinate activities among the different law-enforcement agencies supporting SNS operations?			
Have you arranged for law-enforcement officers to escort delivery vehicles and/or to secure key transportation arteries?			
Does your written security plan include an evacuation contingency?			
Have you informed your security-support team that they may also be needed in a natural or technological disaster?			

## Deployment Processes

Process	Responsibility		
	State	Regional	Local
Have you explored the use of alternative transportation methods, such as helicopters, railroads, subways, or waterways, for the distribution of SNS assets?			