

Additional resources may be obtained at the following websites listed on this slide: CSB&EI, APIC, CDC, USAMRIID and Johns Hopkins.

Thank you for participating in this educational program. By participating, you are taking an important first step in helping to prepare our nation for the threat of bioterrorism. I would like to extend a special thank you to Ruth Carrico from the University of Louisville for editing this program.

missteps offer guide to fight next bioterror battle” and presentations made at the National Summit on Bioterrorism Response Strategies in Washington, DC, in January, 2002.

The best in human nature tends to come out in times of crisis such as the airplane attack on the Pentagon in the fall of 2001. Thousands of volunteers showed up at the site of the wreckage and at the American Red Cross building wanting to participate in any way possible. While this was appreciated, it was also a huge logistical issue and security risk. Thousands of people were flooding the crime scene and there was not an organized way to screen or control the volunteers.

In addition, hundreds of residents and restaurants brought food to the wreck site to help feed the workers. Unfortunately, this is a huge public health concern because improperly prepared or stored food can lead to food-borne illness. Again, the volunteers that brought the food needed to be screened by law enforcement and a control process needed to be created to keep track of people, vehicles and equipment.

The Red Cross had a similar problem trying to control and screen the thousands of volunteers that showed up on their doorstep willing to help. Some volunteered to donate blood while others, such as physicians and nurses, offered up their medical expertise. While this was very generous and helpful, it also posed a huge coordination and security problem. I think it’s safe to assume this same scenario would occur following a bioterrorism attack. Nurses and physicians will want to help and may flood local hospitals in an effort to be of assistance. Security processes will need to be in place to keep track of these volunteers and direct people where to go.

Another important lesson learned from the Pentagon attack is that the media will take over any available space if there is not a designated area for them. Space and spokespeople for the media need to be determined as part of the planning process and not wait until an incident occurs to find a solution.

Many of the lessons learned from the anthrax contaminated letter incidents concerned media management and the importance of an effective communications network. The public was very frightened and needed accurate information in a timely fashion. Both the media and the public demanded a constant stream of information, something for which we were unprepared. The communication network established prior to these events was inadequate to handle the media demands. According to DA Henderson, the requests for information “just buried us in a way we had not anticipated.”

Due to the high demand for information and the reluctance on the part of some agencies to provide information, the media turned to self-proclaimed experts. Problems arose when some of these experts provided misleading or incorrect information, which heightened the confusion and panic in the public. It is important to note that this will happen in future situations if we are not prepared to step up as experts and provide a consistent, accurate message to the public.

In addition to the media demands, interagency communication was problematic following the anthrax letter incidents. Many of the responding agencies were unaccustomed to working together. Miscommunication occurred due to profession-specific jargon that needed to be explained and interpreted in order for each group to understand the other.

One example of this is the difficulty between law enforcement and the medical profession. Prior to the these incidents, their interactions had been limited. They needed to learn to assist each other and work together rapidly in order to mount an effective response. The FBI had to learn to collect evidence without disturbing the medical process and physicians had to learn to treat patients without disturbing the chain of custody process. These miscommunications occurred between agencies as well as between professions.

This quote from Julie Gerberding sums it up well, “We were certainly not prepared for layers and levels of collaboration” among a vast array of government agencies and professional organizations “that would be required to be efficient and successful” in the anthrax outbreak.

Now that we have learned valuable lessons from these experiences, it is imperative that we apply these lessons to training initiatives and incorporate them into our response plans so that we are better prepared for future incidents.

- Foundation of common terminology
- Flexible modular organization that allows for expansion and contraction
- Integrated communications consisting of shared communications plan and standard operating procedures
- Designated leader to which everyone reports
- Unified command structure consisting of a set of shared objectives and strategies
- Manageable span of control meaning the number and list of resources any supervisor may control
- Designated incident facility which may include a staging area and/or more than one facility and
- Comprehensive resource management

An excellent model for the incident command system has been developed by the San Mateo County Health Services Agency in California. This is a comprehensive Incident Command System called the Hospital Emergency Incident Command System or HEICS. HEICS is based on the Incident Command System (ICS), but was designed to be specific for healthcare facilities, most notably hospitals. It functions as a framework for communication and delineation of the lines of authority during a disaster.

HEICS provides an organizational chart with positions that have specific missions to address during the emergency situation. Each position is given a job action sheet that describes responsibilities assigned to that individual. HEICS has been incorporated into the Disaster Plan Checklist mentioned earlier in this presentation; in addition, it is a component of the APIC Planning Suggestions for Bioterrorism Preparedness. You may obtain a HEICS manual or additional information from the San Mateo County website at: www.emsa.cahwnet.gov/dms2/heics3.htm.

It should be noted that version 4 of HEICS is currently underway, but is not yet available. Important changes, such as re-arranging the Medical Staff Officer position, are to be included. If your facility chooses to use HEICS, you should check back with the website regularly for updates to the system.

When deciding whether to incorporate a traditional incident command system or HEICS into your facility's plan, keep in mind that this is a community-wide reporting and communications structure. It is best to use the system that your community has chosen as its standard. If other hospitals in your area are using HEICS, it would be best if your facility also uses HEICS. This will cut down on miscommunication, which could result in a delayed or ineffective response.

One final component of communication involves interaction with the media. Your relationship with the media will greatly impact the effectiveness of your response. The media provides an ideal outlet for sharing important treatment and prophylaxis information as well as updates on progression of events.

It is best to designate only one spokesperson, or one spokesperson for each shift, that will interact with the media. Keep in mind that the media requests for information will be nonstop 24/7. The spokesperson or people need to be informed, educated, articulate and calm. The spokesperson/people should be designated prior to a crisis and it is best if the person is not assigned other duties critical to management of the crisis. In the midst of the crisis, it would be a huge problem just to find someone who knows what's going on and isn't too busy managing the emergency to explain it.

It is imperative to get a consistent, accurate message to the public. The public will need to know who is at risk, how to access medical treatment and how to protect themselves. Try to restrict people other than the designated spokesperson or people from speaking to the media in order to prevent the sending of mixed messages which may result in confusion and panic in your community. Messages should be planned in advance and, if possible, have written answers or fact sheets readily available. This will not only make the spokesperson more comfortable, but it will also provide the media an accurate reference to which they may refer in future reports.

Due to the need for short newsbytes and to avoid being misquoted, spokespersons should be instructed to avoid speculations. Only verified facts in short, easy to understand terminology should be provided to the media. In addition, it is imperative that the spokesperson or people need to rehearse. Mock interviews should be incorporated as part of your facility's exercise program. One option is to videotape the mock interviews so that participants can critique their own performance and identify opportunities for improvement.

I would like to conclude with a few slides on lessons that we have learned from the Pentagon attack and the anthrax letters incident. This information is taken from an article in the New York Times entitled, "Anthrax

them back to normal operations. Consequence management will involve handling the victims, resource management, and other recovery efforts.

This slide illustrates the chain of command for both crisis and consequence management. Crisis management is depicted on the left side of the slide; consequence management is on the right. Not only does this slide illustrate how reporting and communication occurs within the lead federal agency, depicted by the black lines, but it also demonstrates the informal communication that must occur between the FBI and FEMA. This informal reporting and communication structure is depicted by the dotted lines. It will be imperative that the FBI and FEMA communicate with each other in the event of a bioterrorism attack. It is also critical that these federal agencies coordinate their plans and efforts in order to maximize the response.

In addition to the communication structure outlined in crisis and consequence management, communication and reporting will be vital within your facility and with outside agencies. This may include other healthcare facilities in your healthcare system or community. All healthcare and public health facilities and agencies need to have a communications network in place before an incident occurs to maximize an effective response. Building this communications network will require the formation of key partnerships both within your organization and with outside agencies. The process of developing and exercising the response plan will aid in this endeavor.

The following is a partial list of groups with which you need to partner before an event occurs:

- Public Health
- Hospital Epidemiologist
- Infectious Diseases
- Environmental Health
- Emergency Department
- Security
- Facilities Engineering
- Your hospital/facility administrator
- Emergency Medical Service Personnel
- Law Enforcement
- Local FBI

During the implementation of the response plan, reporting and communication will take place within an incident command framework. Under this system, specific roles are assigned to individuals and a distinct chain of command comes into effect. Individuals may be responsible for areas and personnel new to them. Specific job responsibilities are provided and everyone is expected to perform their job within defined parameters and within specific command structures. For instance, an ICP may be assigned a role in the incident command system, requiring new job responsibilities and a new reporting structure. In other words, the ICP would report to the Incident Commander rather than his/her usual supervisor.

Most Infection Control Professionals and other healthcare employees are not familiar with incident command or the terminology and structure upon which it is based. It is imperative that you become familiar with the system before an incident occurs as it will be the communication structure implemented during a large-scale emergency such as a bioterrorism event. It will be easier to learn this system before a crisis occurs rather than trying to learn the system during a time of chaos.

The Incident Command System, or ICS, consists of basic operating principles that ensure rapid and appropriate resource management while aiming to continue routine operating procedures of the organization. In other words, ICS would need to be implemented to mitigate the consequences of a bioterrorism event, while maintaining as many of the day-to-day duties of the facility as possible.

An Incident Command System consists of the following components:

- Command
- Planning
- Operations
- Logistics and
- Finance/Administration

The primary principles involved in the Incident Command System include the following:

most healthcare professionals; forming partnerships with federal agencies in advance will build a relationship and communications network that will make working together easier in the time of crisis. One of the most important things to keep in mind is to rapidly institute the reporting structure if you suspect a bioterrorism attack. The earlier the local and state health departments become involved and notify the FBI, the more likely it is that critical evidence will be obtained and conserved. For example, if you have a patient that you suspect has anthrax, you wouldn't want to treat them and release them before involving the health departments and FBI. There may be additional clinical samples or information that needs to be collected during the initial exam in order to facilitate the criminal investigation.

The last two issues involved in the response phase are flexibility and remaining calm. These two things go hand in hand. It is imperative that healthcare workers remain professional. As always, patients, patients' families, visitors, and the community will count on healthcare professionals to remain calm and in control. Panic will not help the situation. Staying focused and in control will allow for better implementation of the response plan, resulting in saved lives.

In addition, it is imperative that we remain flexible during this time. In the event of a large-scale bioterrorism attack, there will be a time of adjustment during implementation of the response plan. This most likely will alter normal procedures for a short period of time. For example, ICP's may be reassigned to any number of different areas to assist in mitigation of the disaster. One such area may include direct patient care areas in order to meet the high demands for rapid care of new cases and longer-term care for survivors. Be prepared to assist in whatever capacity your facility or community will require. As mentioned previously, a component of the emergency management model is continuity of the organization. This means that it is a primary goal to return to normal operating procedures as soon as possible in order to maintain the integrity of the healthcare system. Your professional composure and flexibility during the time of crisis will be crucial to achieving this goal.

Let's now turn to organization of the response plan implementation. How will the response look? Who will be in charge? To whom should you report? How will communication take place and with whom do we need to communicate? Let's begin with the reporting structure both in terms of reporting a potential incident and the reporting structure during implementation of the response plan.

The CDC designed an algorithm to depict the appropriate reporting structure; this algorithm is available at their website: www.cdc.gov. The original algorithm begins at the point of contact with the health department. Because of this, CSB&EI designed an updated version of the algorithm from a healthcare provider's perspective. This slide shows the algorithm, but due to font restrictions, you cannot read the writing. To make it easier to read, I have enlarged the reporting responsibilities section on the next slide, but before we go there, I want to cover the big picture of the reporting structure. In a nutshell, the reporting structure indicates that if a bioterrorism attack is suspected or known, healthcare workers should first contact their local health department. A full-page legible version of this algorithm is available to download or print from the CSB&EI website listed on this slide or in the reference section of this program.

This slide shows an enlarged version of the reporting algorithm from the previous slide. Please note that the text boxes have been switched from horizontal to vertical to make it easier to read. The top box begins with the reporting responsibilities of the healthcare provider. It is the healthcare provider's responsibility to notify the local health department and any other people or groups identified in the facility's response plan. This may include Infection Control, Hospital Epidemiologist, Infectious Disease physician or department, administrator on duty, etc. Each facility needs to decide who should be notified and include this list in their response plan. Once the local health department has been notified, it is their responsibility to investigate and contact the state health department, local law enforcement and the FBI if the event is deemed credible. Lastly, the state health department is responsible for contacting the CDC.

Once the response plan is initiated, who will be in charge? It depends on whether the organization is in the crisis or consequence management component of the response. In the Crisis Management phase of response, the FBI is the lead federal agency. The ultimate goal of crisis management is to capture the perpetrators and prevent additional attacks.

During Consequence Management, FEMA becomes the lead federal agency in charge. The ultimate goal of consequence management is to manage and minimize the impact of the event on the community and returning

by implementing droplet isolation for coughing patients until a causative agent is identified. Once you have ruled out a contagious agent, such as pneumonic plague, isolation can be discontinued.

This also means that isolation should not be discontinued until strain resistance is verified. It is possible that terrorists will release genetically altered strains of organisms. For example, the usual recommendation is to discontinue droplet isolation after 48 hours of antibiotic therapy in patients with pneumonic plague, but if the patient is infected with a genetically resistant strain, discontinuation of isolation could result in exposure to other patients and staff. Isolation should never be discontinued until the patient meets all criteria such as 48 hours of antibiotics and they are showing signs of clinical improvement. It is better to over-isolate than risk nosocomial transmission.

If you are at risk from exposure to the primary source or secondary spread, you need to follow appropriate medical recommendations, including treatment, prophylaxis or vaccination as indicated. Prompt initiation of treatment, prophylaxis and/or vaccination will be critical in the prevention of morbidity and mortality. Following a bioterrorism attack, it will be imperative to keep all healthcare and public health professionals healthy and able to work. This is important not only for the healthcare facility for which you work, but also for your family and your community. You don't want to spread illness to your family who in turn may spread it within your community.

Another issue that will need to be addressed during the response phase is decontamination, both in terms of patient and environmental decontamination. The extent of decontamination needed is entirely scenario-driven. The scope of the release, the agent used, and the length of time from release to identification of attack will all impact the decontamination interventions necessary to control secondary spread.

Let's start with patient decontamination and then progress to environmental decontamination since the recommendations vary depending on the source you are attempting to decontaminate. Decontamination recommendations will vary depending on how soon the release is identified. For example, in the event of a covert release of a biological agent, patient decontamination may not be necessary. By the time patients become symptomatic and present to healthcare institutions days to weeks after the exposure, patients will most likely have bathed and changed their clothes. This means that they have already decontaminated themselves.

However, if the attack is announced (within 12-24 hours after the release), exposed individuals should be decontaminated by bathing them with plain soap and water and changing their clothing. Bleach, Lysol, and other harsh chemicals are not needed and should be avoided since they are skin irritants.

Environmental decontamination recommendations depend upon the location of the environmental source of concern, agent utilized and the scope of the release.

Based on existing knowledge, decontamination is not considered necessary for streets, cars or the outside of buildings. This is due to the fact that weather plays a key role in rapidly disseminating biological agents in outside air.

Indoor environmental sources will require decontamination strategies, but the interventions vary depending on the agent utilized and the scope of the release. For example, more stringent decontamination methods are necessary for anthrax when it is released in spore form, due to the hardy nature of spores. Final recommendations regarding environmental decontamination following release of anthrax are pending investigation into the anthrax letters that contaminated postal offices in the fall of 2001.

Other agents require diligent environmental decontamination as well, such as smallpox. Smallpox can be spread by hand to hand contact or contact with fomites, making decontamination of environmental surfaces imperative to prevent secondary transmission. Only EPA-registered, healthcare facility-approved disinfectants are required for environmental decontamination of smallpox, although a 0.5% hypochlorite solution may be used. This solution is made by mixing one part household bleach with nine parts water. In the event of a single smallpox case, decontamination of the inside of your healthcare facility would be critical to prevent secondary spread. Decontamination recommendations for other biological agents are available in training products that cover treatment and patient management of potential bioterrorism agents.

Another important component of the response phase is assisting in the criminal investigation. Bioterrorism is a crime and will be extensively investigated by the FBI. As part of the investigation, the FBI will be gathering evidence, requiring participation from both healthcare and public health agencies. These procedures are new to

Assume your ER has 33 patients arrive on the same day with symptoms of severe, rapidly progressing pneumonia that resulted in death within 24 hours of admission. This scenario provides many issues that would need to be addressed during the exercise. Some examples of issues that would be addressed in this drill might include:

- Should isolation be used
- Should prophylaxis be provided before the agent is identified, and if so, who should receive it
- How can the hospital handle the influx of current and potential future patients
- What should be said, if anything, to the media before concrete information is known and
- At what point should the incident command system be initiated.

While scenarios are helpful in creating a frame of reference from which to begin an emergency response plan, they should not be limited to frightening stories of the chaos that would occur following an overwhelming bioterrorism attack. The goals are to identify gaps in the plan and get the key personnel together discussing the issues. This should result in a more thorough response plan and an effective communication structure with which to implement the plan.

That concludes the preparedness phase of the emergency management model. Let's now turn to the response phase and discuss the ICP's role. As mentioned previously, the response phase consists of patient management and effective communication.

Regardless of the size of the release, patient management will be a major issue in the response phase. However, the scope of the release will greatly impact the type of interventions necessary for patient management. A large release of a contagious agent will place different demands on a facility than a small release of a non-infectious agent.

One of the first components of patient management will be the need to rapidly and accurately identify the causative agent. Treatment, prophylaxis and isolation all depend upon the causative agent. Time is of the essence because some of these agents can progress to death very rapidly without appropriate treatment. For example, untreated pneumonic plague usually progresses to death within 36 – 72 hours.

Agent identification and patient diagnosis will depend a great deal on the treating clinician's high index of suspicion and knowledge and familiarity with the potential bioterrorism agents. Obtaining an accurate assessment and patient history will also be critical.

The history should include symptoms, severity of illness, date of symptom onset, source, route, location, and date of exposure if known, and body site affected. For example, a new onset of a painless necrotic lesion on the arm might indicate cutaneous anthrax while respiratory symptoms with an accompanying widened mediastinum on chest x-ray would imply inhalational anthrax. Both diseases result from exposure to the same agent, but the route of exposure is different.

Date of symptom onset will be important in order to determine approximate date of exposure, which may lead you to the location and date of the release. This will require epidemiological investigative skills to determine the source, route, location and date of exposure. While this information will not help the patient you are currently treating, it may prevent future deaths by identifying other high-risk groups that would benefit from prophylaxis.

Once the initial case or cases have been identified, a sentinel surveillance program should be instituted to identify additional cases. Sentinel surveillance is simply an active surveillance program which is initiated in response to a sentinel event, in this case, a bioterrorism attack. For example, if a patient presents to your facility with pneumonic plague suspected as having resulted from an intentional release, an active surveillance program should be implemented to rapidly identify additional cases that present to your facility. Communication will be critical to the success of this surveillance program and community-wide implementation of sentinel surveillance is encouraged once a single case is identified in a community.

Protection is a key element in patient management. By protection, I mean protecting the patient you are treating, other patients in your facility, visitors, staff, and yourself. This includes people both within your facility and in your community, including your family. The steps you take can protect your community or put you at risk.

What can we do to protect our community and ourselves? First of all, you should take a conservative approach to any interventions. Rapid and appropriate isolation is imperative. You should err on the side of caution

The scenario consists of a “story” in which an agent, location of release and weather conditions are chosen and the expected outcome of the fictional “release” is reported. The advantage to using a scenario is that it provides an element of realism and attempts to draw the participating groups into the situation, similar to the use of case presentations versus teaching from theory.

The third step in an exercise program is a drill. A drill is an emergency response function in which an organization physically works through a scenario. In general, drills focus on a limited part of the response plan and may or may not involve a field component. Drills only involve one facility and do not incorporate interagency communication or cooperation.

The fourth step in an exercise program is a functional exercise. In essence they are expanded versions of a tabletop. Functional exercises are realistic practice of a response plan that takes place in real time at the emergency operations center or EOC. Participants assume their real-life roles they would play in an emergency while a narrator reads a scenario out loud to direct the progression of the exercise. One example is having participants act as citizens that call and demand information about where to obtain prophylaxis following a media announcement that anthrax has been released in the community. Participants must respond to developments in the scenario without prewritten scripts. These exercises tend to be stressful due to time pressure and the realistic nature of the exercise.

The final step in an exercise program is a full-scale exercise. Full-scale exercises are elaborate events involving actual mobilization of people and resources in a multiple-agency exercise that take place in real time. The EOC is activated and real people, equipment and supplies are used. Full-scale exercises require a great deal of upfront planning as well as a financial investment.

The different types and levels that make up an exercise programs are designed to be implemented incrementally. These exercises are progressive, meaning that each step builds upon the other. Facilities or communities should not expect to jump into a full-scale exercise without first performing an orientation, tabletop, drill and functional exercise.

FEMA provides a sample program with accompanying timeline for communities looking to implement an exercise program. One example would be an orientation at 1 month, a tabletop at 4 months, another orientation to discuss the tabletop and updates to the plan at 7 months, a single agency drill at 9 months, a tabletop at 11 months, a functional exercise at 14 months and a full-scale community exercise at 18 months. Some facilities or communities may need to adjust the timeline to fit their needs.

The incorporation of scenarios into an exercise program is critical. In the past, scenarios have received some criticism due to the tendency to estimate a large release as part of the exercise. Some argue that these scenarios do little more than scare and overwhelm the participants in the exercise and lead to inertia in the group due to the feeling that adequate preparation is too difficult a task. Advocates for the use of scenarios argue that the purpose of scenarios, regardless of the exercise’s estimated release size, is to raise awareness and identify gaps in the planning process in order to address those before an actual event occurs.

Because of this, many community teams are starting their planning process with an assumed number of casualties from a specified agent to determine if their community can handle that influx of patients. For instance, a planning team may decide to develop a plan that can handle at least 100 casualties with a non-contagious agent. While this would not be adequate to prepare a facility for a large-scale release, it at least provides the community with a starting point and ensures that the proper communication and framework are in place to handle a release of any size.

The advantage to using a scenario is that it furnishes the participants a framework from which to understand the myriad of issues surrounding a bioterrorism response plan. Lack of dedicated decontamination areas, number of isolation rooms, supplies, medications and delivery methods for prophylaxis are just a few of the gaps that may need to be addressed by your facility. If the scenario included a contagious agent, such as plague, it becomes even more complicated trying to incorporate resources needed for isolation and ventilatory support for victims.

related to a bioterrorism event. However, state or federal resources are no use to a facility or community unless these resources are made available at the local level. In order to access these resources, facilities and communities need to be aware of what type of resources are available and how to access them.

One such example is the National Pharmaceutical Stockpile. The stockpile's mission is to "ensure the availability of life-saving pharmaceuticals, antibiotics, chemical interventions, as well as medical, surgical, and patient support supplies, and equipment for prompt delivery to the site of a disaster". The primary goal is to provide necessary antibiotics, medications, vaccines, and medical supplies to the affected community in a very short period of time. The exact contents of the stockpile are not disclosed for security purposes, but will contain medications and vaccines needed to treat and/or prophylax the primary bioterrorism and chemical terrorism agents of concern.

The National Pharmaceutical Stockpile consists of two components: 12 hour push packages and Vendor Managed Inventory (VMI). The push packages consist of a preassembled set of supplies, pharmaceuticals and medical supplies that are maintained in warehouses spread across the United States for easy distribution. A distribution system has been designed so that the push packets can be made available to any affected area within 12 hours of authorization for release. These packages have appropriate contents to treat a variety of different agents, even if the causative agent has not yet been identified. The goal of the push packets is to provide broad coverage for short-term use until the causative agent has been identified.

Once the causative agent is identified, which usually requires 24 – 36 hours, the Vendor Managed Inventory packages may be accessed. The advantage to the VMI packages is that they can be agent-specific or used to respond to a larger or multi-phased attack. Further information on the National Pharmaceutical Stockpile may be found at CDC's website: <http://www.bt.cdc.gov/>.

Once the initial version of the plan is developed and staff are educated on the plan, how do we assess preparedness? How do we measure the effectiveness of the plan? What performance and outcome measurement tools are available for these assessments? An evaluation of the effectiveness of preparedness plans at the health care facility and community levels are an integral component of effective planning. Healthcare and regulatory agencies require performance-based evaluation. Performance measurement of bioterrorism preparedness must, therefore, be integrated into emergency management plans.

Where do we find performance measurement tools to evaluate our preparedness plans? Currently, there are no standardized, validated performance measurement tools to assess bioterrorism preparedness. Most facilities and communities use subjective evaluations of the outcomes of exercises and drills to determine bioterrorism preparedness. Although scenarios for exercises are not standardized and may be modified to fit the needs of particular groups, components of these exercises can be standardized. Evaluation tools can then be developed to be used across various facility and community plans to identify gaps in preparedness.

Exercising your response plan provides many benefits to you and your facility or community. One of the most important reasons to exercise your plan is that it will help identify weaknesses in your plan that can be corrected before an incident occurs. In addition, gaps in resources may be identified, participants' roles and responsibilities are clarified and coordination between internal and external agencies is enhanced.

Exercise programs can make the difference between a poor and an effective response, which will translate into lives and resources saved. In addition, some regulatory agencies, including the Joint Commission on Accreditation of Healthcare Organizations or JCAHO, require annual execution of the plan in the form of a natural event or planned drill. One example of an exercise program is one created by the Federal Emergency Management Agency, or FEMA. FEMA's exercise program is composed of a five stage process of exercises which increase intensity and realism as you progress through the program. The five types of exercises include orientation, table top, drill, functional and full-scale drills.

The orientation drill is an informal exercise in which participants get together and discuss preparedness plans. There is no simulation of an event and a scenario is not utilized. The primary purpose is communication and partnership development.

The tabletop exercise is the second step in an exercise program. A tabletop is an informal discussion, which is paced slowly and should take place in a low stress environment. Unlike orientations, tabletops usually involve a scenario.

resources and identify sources to obtain additional resources before an incident occurs. If you wait until the crisis, the delay required to obtain additional resources could result in a higher mortality rate.

Facility assessment should also involve the assessment of the current communication system. Is it effective? Can departments communicate between themselves and with outside agencies? Do you have a back-up plan in case of an emergency? Auxiliary power and secondary sites need to be established prior to an incident and individuals need to be trained on how to use the system.

In addition to identifying available resources and verifying the existing communication network, facility assessment will aid in development of critical partnerships that need to be in place before a response plan is implemented. The assessment process will help to raise awareness of the potential threat of bioterrorism as well as strengthening relationships within your facility and between your facility and community agencies.

Assessment of a facility for bioterrorism preparedness is a necessary, but complicated task. To thoroughly assess your facility, a multidisciplinary approach must be utilized. Facility assessment and development of an effective response plan will need to be accomplished through communication and coordination with every department within your facility.

Key groups that should work together include Infection Control, Hospital Epidemiologist, Infectious Diseases, administration, laboratory, security, facilities engineering, nursing, pharmacy, Occupational Health, mortuary, respiratory therapy, central supply, housekeeping, and food and nutrition. Other departments or groups may need to be involved; each facility should evaluate their organizational structure and determine key groups that need to participate.

In some facilities, the ICP may be designated as the person responsible for coordination of this assessment. The exact role of the ICP in this process may vary depending upon the needs of the facility. Regardless of whether or not you are the designated coordinator for facility assessment, you should play an active role in this process.

Assessing your facility should be accomplished in an organized method using a standardized tool such as the Facility Mass Casualty Disaster Plan Checklist: A Template for Healthcare Facilities. This checklist is an addendum to the APIC/CDC Planning Template and can be found on APIC or CSB&EI's website.

A second option is to incorporate the assessment into the response plan exercise program for the facility. These exercise programs will be discussed in greater detail later in this presentation. Ideally, a facility would use the Disaster Plan Checklist to assess their facility as part of the facility's exercise program.

The foundation for the Facility Mass Casualty Disaster Plan Checklist was originally created by the New South Wales Department of Health Counter Disaster Unit in preparation for the 2000 Olympic Games that took place in Sydney, Australia. The Counter Disaster Unit was kind enough to share this document with CSB&EI. The document was then modified by the APIC Bioterrorism Task Force and has since become a CSB&EI and APIC document.

The Disaster Plan Checklist is a template designed to assess a facility in preparation for an intentional or natural incident that results in mass casualties. The Disaster Plan Checklist incorporates elements of emergency management such as mitigation, preparedness, response and recovery and is ideal as a foundation for development of a preparedness plan for bioterrorism. The Disaster Plan Checklist is an eighteen page comprehensive document composed of twenty-five sections. Each section has a series of questions that need to be evaluated as to whether the objective has been met, action plan to fill gaps that are identified and the person responsible for filling those gaps or maintaining the objective.

Many of the sections overlap and affect numerous departments within the facility as well as outside agencies that should be working with the facility to develop a response plan. As mentioned previously, the Disaster Plan Checklist is not meant to be filled out by an individual working alone; it is designed to spark communication and development of partnerships throughout the facility and between the entity and outside agencies. Questions and sections may need to be added or amended to meet the needs of the assessing facility.

In addition to on-hand resources and back-up resources available from a facility's community, resources will be made available from state and federal agencies. These resources will be imperative to reduce the loss of life

September 11th, telephone and cell phone lines can easily become clogged and subsequently are unavailable. Clogged phone lines results not only in the loss of phone service, but also access to faxes and the internet. This may mean that your facility is on its own in terms of obtaining expert advice. The best solution to this is to have resource materials on hand in either CD-ROM or written formats, or keep copies on your hard drive so that you can still access these materials in the event of loss of telephone service.

The development and assessment of a facility bioterrorism response plan needs to be undertaken either before or in conjunction with staff training. It is important to note that these are all ongoing processes and not tasks that are completed once and then abandoned. A facility's response plan should always be considered a work in progress. Additions and updates are made as gaps are identified and policy changes emerge. Furthermore, these changes to the plan must be communicated to the staff; response plans are only as effective as the staff implementing them.

Each facility's response plan development committee needs to appoint an individual that will be responsible for coordinating the writing of the plan. In some facilities this may be the Infection Control Professional, but it could also be the Hospital Epidemiologist, an Infectious Disease physician, emergency management leader, environmental health professional or other knowledgeable individual.

Although one person is generally responsible for coordination of the written plan, the actual development of the plan needs to be multi-departmental. Regardless of who is assigned the role of coordinator, the ICP needs to play a critical role in the response plan development team.

In addition to playing a critical role in the development of the facility bioterrorism response plan, the ICP should be familiar with the plan and know what to expect during the response phase. This also requires you to know your role in the plan. During the time of crisis, it is likely that your facility will implement a new temporary reporting and communication structure, such as the incident command system. If this occurs, you may be assigned a job action sheet that contains duties that are different from day to day operations and you will most likely report to someone other than your usual supervisor. In order to maximize the effectiveness of your facility's disaster plan, it is best if all participants know their role and responsibilities in advance.

One of the easiest and most productive ways of learning your role in a disaster plan is to participate in preparedness initiatives, including the development and assessment of the plan itself. People who write or help develop the plan will be the ones most familiar and comfortable with the implementation. In addition to assisting with the writing or development of the plan, it is imperative that you participate in any exercises that take place in your facility or community. Exercises demonstrate first-hand how implementation of the plan will occur, it allows participants to try out their assigned responsibilities, and introduces the participants to the new reporting and communication structure.

In Israel, hospitals hold approximately 20 drills each year. Each drill focuses on a different type of emergency and the scenarios are rotated so that staff is exposed to a variety of exercises. Types of drills include floods, bombings, chemical terrorism and bioterrorism attacks. Because of this, the hospital staff is familiar with their plans and knows how to handle a variety of different types of disasters.

Development of a bioterrorism response plan is a multi-disciplinary and multiple-step endeavor. One of the first steps in development of a bioterrorism response plan is facility assessment. This assessment has two primary goals. The first goal is to determine on-hand resources. Knowing your facility's baseline of available resources will help determine gaps that need to be filled before a bioterrorism incident occurs. The second goal of facility assessment involves the evaluation of current communication networks.

Quantifying your available resources includes knowing how much functional medical equipment you have on-hand, how much back-up equipment you can obtain and from which sources, your current staffing levels, sources and amount of back-up staff you could obtain in an emergency, the number of licensed and available beds, and the number of beds you could fill in the time of crisis.

One example is assessing the number of functioning ventilators your facility has available on an average day. How many extra ventilators exist in your facility? Do you have enough trained staff to cover the shifts if you increase the number of ventilated patients? Do you know where and how to obtain additional machines and staff? These are just a few of the resources that need to be assessed. It's critical to determine a baseline of available

For the sake of this scenario, let's assume you suspected bioterrorism from the moment they presented to the ER; thus you would receive lab confirmation that the patient had *bacillus anthracis* on Wednesday, one day after the patient has died. Based on the patient's symptoms, you diagnose the patient as having died of inhalational anthrax.

During the patient history, the family tells you that patient's symptoms began approximately five days before the patient presented to the ER. The patient's symptoms had been mild at first and gradually worsened until the point that the patient was having difficulty breathing. It is this symptom that precipitated the trip to the ER.

The incubation period for inhalational anthrax ranges from 1 – 10 days, and can be as much as 43 days after exposure. Assuming it was a large aerosol release and since this is the first patient to present with disease, you can deduce that the exposure probably occurred in the last 1 – 10 days. Furthermore, you should assume that others are potentially at risk of exposure from the same source as the patient. The next step would be to get a history from the family concerning everywhere the patient had been during the incubation period in order to determine the possible location and date of the exposure.

Knowing that the incubation period is most likely the previous 1 – 10 days, you can therefore focus the patient history on that time period. You would need to find out everywhere the patient visited during those 10 days in order to determine the date and location of the release. This information will be critical in identifying others at risk.

For the sake of this example, let's assume the family tells you that the patient has been to the following places only: work, the grocery store, child's school and a baseball game. One thing you need to consider is whether or not to prophylax the community while you're conducting the investigation. If you choose to distribute prophylax, to whom do you provide it? Everyone in the community or only those that have been to the same places as the victim during the last 1 – 10 days?

The date and location of release will be easier to determine if you have more than one victim. This is because with multiple victims, you can compare patient histories and try to narrow the possible source of exposure. For instance, let's assume a second patient presents on the Tuesday that the index case dies. You can now compare the second patient's history with the index cases' to determine if there are any shared places the two victims visited during the incubation period.

This slide shows two schedules: the top timeline shows the places that the index case visited during the incubation period; the bottom timeline indicates the places that the 2nd victim visited. Assuming that the two victims worked in different settings, you can see that the only other common event is the baseball game on the Saturday before the index case became ill. You can conclude from this that the likely source of exposure was the baseball game. Since inhalational anthrax is not contagious, you can now narrow the list of potentially exposed individuals, which may require prophylaxis, to only those people that attended the ballgame or the surrounding area on Saturday.

The Infection Control Professional has the epidemiological skills necessary for performing or assisting in this investigation. Communication is key in this situation, as the health department will most likely be in charge of the investigation with the ICP functioning as a collaborative partner. In the early stages of the investigation and in some communities, the ICP may be responsible for the investigation. The ICP's role should be outlined in your facility and/or community bioterrorism response plan.

Many resources are available for education and training on the potential bioterrorism agents. A few examples include fact sheets, treatment algorithms, isolation guidelines, and a one hour educational program on clinical management of anthrax, smallpox and plague that is available in CD-ROM or video format that can be found at our website, www.bioterrorism.slu.edu. The APIC Bioterrorism Toolkit II which is current as of March, 2002 and will be updated periodically, is available at either the CSBEI or APIC website. In addition, the APIC e-learning website provides many opportunities for education on bioterrorism. Other sources include the CDC and Johns Hopkins' websites. A list of links is available in the reference section of this program.

It is not necessary to memorize all of the patient management information. However, it is critical that you have a basic understanding of how these diseases typically present so that you maintain a high index of suspicion and are on alert for any changes in your medical community. In addition, it is crucial that you identify, in advance, reliable sources of information to which you can refer in a time of crisis. During emergency situations, such as

At my previous job as an Infection Control Specialist at a large hospital, I felt that I had a pretty good handle on the baseline of disease for most of my inpatient population. However, I had no idea of the baseline of respiratory illness seen in the ER or in the outpatient setting. I feel comfortable asserting that most ER's and outpatient clinics could not accurately identify their baseline rate, either. And yet this is something I would have needed to know in order to set up an effective real time syndromic surveillance program for my facility.

Because of the reasons I've listed, you can see why it is so difficult to establish a baseline of disease in your facility or medical community. There are no hard and fast rules for this in relation to bioterrorism. Everyone needs to decide for himself or herself how best to accomplish this. The key here is to be able to quickly identify a subtle change or trend in your population. Even if you can't establish a proven increased rate in some predetermined collection criteria, it is important to notify the health department immediately of any change or trend you think you are seeing in your population. It is better to have a low threshold for alarm rather than miss what may be the beginning wave of patients presenting from a bioterrorism attack.

Another piece of early detection involves being familiar with the most likely agents to be used in a bioterrorism attack. You need to know the clinical presentation, mode of transmission and patient treatment and management. In the event of a sudden surge of ill patients in which your facility surmises may be related to a bioterrorism attack, you still need to rapidly identify the causative agent in order to provide appropriate treatment and isolation. So, while early detection is important, accurate diagnosis of the causative agent will be critical to the success of the response.

As mentioned previously, there are potentially thousands of agents that could be used in a bioterrorism attack. However, the CDC narrowed the list into three categories: A, B and C. Category A agents are the agents considered most likely to occur in a bioterrorism attack. There are 6 Category A agents: anthrax, smallpox, plague, tularemia, botulism and viral hemorrhagic fevers. The list of Category B and C agents may be found at the following CDC website: <http://www.bt.cdc.gov/Agent/Agentlist.asp>.

Similar to the CDC list, the FBI has developed their own list of agents, which are likely to be used in a bioterrorism attack. Some of these agents, such as anthrax, botulism and ricin, are included on both lists. Other agents, such as salmonella and shigella, are included on the FBI list, but are not specifically named in the CDC categories. However, the CDC does include the broad group entitled "food-borne agents" in their Category B list. The FBI purposely lists out salmonella and shigella since they have been used as in bioterrorism activity previously.

It is important to note that organisms such as salmonella and shigella can be used as bioterrorism agents. These organisms are typically the causative agents in naturally occurring food-borne illness outbreaks and may not be suspected as being intentionally released unless you maintain a high index of suspicion and thoroughly investigate the outbreak. This is especially true during summer months when food-borne outbreaks are likely to occur.

When deciding which agents with which you should become familiar, it is important to look at both the CDC and FBI's lists. You should be familiar with all of the CDC Category A agents as well as the FBI's list of most likely bioterrorism agents. Ideally, you should try to become familiar with the CDC's Category B and C agents as well.

In addition to identifying the causative agent, an effective response will require epidemiological skills to identify when and where the release occurred. The date and location of release are critical to determine at-risk groups and, depending on the agent, may determine who needs to be vaccinated and/or prophylaxed.

The patient's history and physical exam should focus on the past and current symptoms, when symptoms first developed, and places the patient had been prior to symptom onset so that the release location and date may be determined.

For example, let's say a patient presents to the ER on a Monday morning with a rapidly progressing sepsis pattern and the patient dies within 24 hrs of admission to the hospital. You most likely wouldn't get the lab results back until Wednesday or Thursday. If you didn't suspect bioterrorism, the diagnosis would be further delayed because confirmatory lab tests for most bioterrorism agents can only be performed at a state health laboratory.

This increase is even more dramatic if you refigure the mean using only the months before the increased rate. In other words, calculate the baseline mean before the increase in September. The mean for the data before September is 6.93, but the mean for the entire set of data was 8.64. Not only do you see a spike in the individual data points, but you also see an increase in the mean by over 2% from baseline

Now plot the two means together on the same graph, with the new mean starting at September, which correlates with the spike in the data. You can now clearly see that there is an increasing trend in the data. When an upward trend or spike is seen in the data, such as September, October and December on the example graph, an investigation is warranted and should be undertaken to determine the cause for the change.

Whenever possible, it is best to initiate the investigation at the first suspicion of an increase. A low threshold of alarm is preferable, even if it means that a few unnecessary investigations are begun; this is preferable to missing an actual event because your threshold for alarm was set too high. Syndromic surveillance is more likely to produce false alarms since you are not tracking a specific indicator of disease. In other words, an increase in ER visits may be related to inclement weather that resulted in numerous car accidents rather than a bioterrorism attack. You will need to begin the investigation to determine the relevance of the data.

While syndromic surveillance provides a good chance of obtaining rapid recognition of a bioterrorism event, it is very resource-intensive. It requires trained, dedicated staff to collect, collate and analyze the data. The chart review required for an effective syndromic surveillance program could translate into an additional half dozen or more FTE's in large facilities. In these days of healthcare cut-backs, extra FTE's are most likely impossible to obtain.

A more cost effective option for performing syndromic surveillance is the use of automated surveillance programs. Unfortunately, while this software is currently being researched, it is not currently available to all facilities. Furthermore, most experts believe that it is more likely that an astute clinician will identify a potential bioterrorism attack rather than our current surveillance mechanisms.

An active surveillance program can be set up and run by the ICP within the facility or in conjunction with the local health department. Alternatively, facilities may choose to participate in a passive surveillance system in cooperation with the local health department. Regardless of which type of surveillance is chosen by a facility or community, the Infection Control Professional plays a vital role in setting up and coordinating the surveillance system as well as analyzing the data and reporting suspected incidents to the local health department. The surveillance process and the necessary corresponding communication network will be essential to the early detection of a bioterrorism attack.

Regardless of whether a facility decides to implement passive or active surveillance, it will be vital to maintain a high index of suspicion. You need to keep the possibility of a bioterrorism attack in the back of your mind. It will be easy to misdiagnose victims of bioterrorism because the symptoms are so similar to other respiratory and flu-like illnesses that commonly occur. This is especially true during influenza season when it is normal to see a large influx of patients with flu-like symptoms. There's an old saying in the medical field, "If you hear hoof beats, think of a horse, not a zebra." In the case of bioterrorism, this is modified slightly to be, "If you hear hoofbeats, think of a horse first, but don't rule out the possibility that it could be a zebra."

Part of maintaining a high index of suspicion and early detection involves knowing your facility or medical community's baseline. If you don't know what's normal in your population, it will be hard to know that there has been a subtle change or trend unless the event is huge. It would be ideal to implement a response plan as early as possible to mitigate the potential consequences and this requires early detection.

Similar to the development of a case definition, determining your baseline as it relates to a bioterrorism attack is a difficult concept. As mentioned previously, other Infection Control issues often have standardized definitions and easily accessible lab tests. With these conditions, it is relatively easy to establish a baseline. Since there are potentially thousands of biological agents that could be used in a bioterrorism attack, you obviously cannot perform active surveillance for all of them. Establishing a baseline for syndromic surveillance is even more overwhelming. How difficult would it be for your facility to track the number of patients presenting with respiratory illnesses?

While tracking and analyzing the number of patients seen in an ER or hospital admissions may not seem like an effective way to perform bioterrorism surveillance, keep in mind that bioterrorism surveillance is, in some ways, unlike traditional surveillance programs. With other Infection Control issues, such as bloodstream infections, you have standardized definitions that are often associated with easily accessible lab tests. Case finding is relatively easy. With bioterrorism, there are countless possible scenarios: the presenting disease could be bacterial, viral or caused by a toxin, the illness may or may not be contagious, and patients usually present with nonspecific flu-like symptoms.

In addition, most of the potential bioterrorism agents cause uncommon diseases, such as inhalational anthrax, tularemia and pneumonic plague, and most facilities do not have the lab capability to test for these illnesses. This makes case finding very difficult. It is best to use available data, such as hospital admissions, to start a surveillance program. Once the program is underway, you can work toward improving the process.

One other option for active surveillance involves the use of syndromic surveillance. Syndromic surveillance consists of collecting and analyzing non-traditional data. Traditionally, syndromic surveillance referred to the collection and analysis of syndrome-related data.

A few examples of traditional syndromic surveillance data include the following:

- Severe flu-like illness indicating the release of inhalational anthrax, pneumonic plague, smallpox or other diseases
- Flaccid muscle paralysis indicating that a neurotoxin, such as botulism toxin, may have been released
- Bleeding disorders indicating the use of a viral hemorrhagic fever agent
- Rash indicating the release of smallpox
- Apparent food-borne illnesses possibly indicating an intentional release on a food source or vendor

Newer attempts at collecting syndromic surveillance data indicate a broader definition for syndromic surveillance. Almost any non-traditional data that may indicate a potential bioterrorism event has occurred may now be classified as syndromic surveillance. A few examples of newer syndromic surveillance data include the following:

- Number of patients presenting to the Emergency department with flu-like illness as their chief complaint
- Number of purchases of over-the-counter flu remedies or
- Number of purchases of over-the-counter diarrhea medications

Surveillance of grocery sales is perhaps one of the most interesting ways to conduct syndromic surveillance. Data is gathered on the number of grocery items purchased that could indicate that patients are experiencing flu-like symptoms, such as orange juice, chicken noodle soup and facial tissues.

The rate of grocery purchases are compared to the rate of physician visits or phone calls with nursing consultation lines. Studies conducted in the New York area indicated that the sales of these products did correlate with an increase in the number of physician visits and healthcare professional phone consultations. Whether this data collection would correlate with a bioterrorism attack has yet to be determined, but I mentioned it because it's a good example of an innovative way of conducting syndromic surveillance.

Regardless of which type of non-traditional data is collected as part of syndromic surveillance, the data is handled and analyzed in a similar manner: rates and means for the data are determined. When a change in the data indicates an upward trend or spike over a pre-determined threshold, an investigation would need to be undertaken. This is similar to other surveillance, such as monitoring the rates of blood stream infections or surgical site infections, conducted daily by Infection Control Professionals.

This is an example of a graph illustrating surveillance data. The numbers on the y axis, the left vertical side of the graph, indicate the number or rate of the indicator for which you are collecting, such as the number of ED visits each day or the rate of bloodstream infections for a month. For this example, I have plotted fictitious monthly rates for bloodstream infections in an ICU.

The numbers on the bottom of the graph, the x axis, indicate the month and year that the indicator occurred. In this example, data was collected starting in January of 2002 and continued through January 2003. Once the number or rate is charted on the graph, the mean, or average, should be calculated and added to the graph. What you'll notice on the graph is that there appears to be an increase in the rate starting around September.

that an unnatural event has occurred. In this scenario, traditional first responders- policemen, firefighters, and EMS- show up at the scene and they triage and take care of the victims, transporting them to the hospitals, etc.

With bioterrorism, it is completely different. There may not be an explosion and we may not know that it has occurred unless the perpetrators announce the attack. The anthrax letters are a good example of a small, announced attack in which traditional first responders are necessary to help control the scene.

In the case of a bioterrorism attack on a large scale where an agent is covertly released in an aerosol form, the response will be different. A few days or weeks after the release, patients will begin to show symptoms and will access the medical system at that point. Most likely these patients will go to an ER or some other primary care facility. There will not be a readily identifiable affected area that we can put a rope around and designate as Ground Zero. Therefore, the traditional first responders will not be as critical as they are during a traditional terrorist attack. In this scenario of a large aerosolized bioterrorism attack, the first responders will be health care and public health professionals.

Critical to an effective bioterrorism response is early detection of an attack. The sooner the attack and at-risk patients are identified, the higher the likelihood of decreasing morbidity, mortality and cost associated with the incident. Early detection may be achieved by two methods: stand off detectors or a surveillance program.

Stand off detectors are machines that function similarly to smoke detectors. They work by drawing in a sample of air and analyzing the content to determine if biological particles are present. The technology in this field is changing rapidly, but the effectiveness of this technology has serious limitations.

While some detectors can determine a biological particle is in the air, most available equipment cannot identify the exact organism. In addition, stand off detectors are quite costly and a city would need many machines to adequately perform surveillance since the detection equipment need to be pre-positioned. Stand off detectors only provide coverage for a limited area. For these reasons, stand off detectors are not very useful for real time surveillance of a city or area. The exception to this is the use of this equipment at a large venue, such as the Super Bowl or the Olympics, in which the detectors can be used effectively to rapidly identify the release of a biological agent in a limited, well-defined area.

This slide shows a picture of a stand off detector developed by Bruker Daltonics.

This slide shows another picture of a stand off detector developed by Bruker Daltonics.

For most communities, the most effective way to ensure early detection is through a surveillance program. Surveillance involves collecting and analyzing data to establish a baseline and determine a point at which there is a change or trend in the health of the population. There are two methods of gathering information in a surveillance program: active and passive data collection.

Passive surveillance involves only the collection of data from unsolicited source reports. In other words, you wait for someone to call and tell you that something has changed in their medical community. In terms of bioterrorism, a passive surveillance system would be one in which the data collector waits for others to report unusual occurrences in the community.

Active surveillance, on the other hand, involves direct solicitation of data from others participating in the active surveillance program. An example of an active surveillance program would be one in which the data collector would contact specified people and/or groups in the community and ask for predetermined information.

Some examples of data that could be collected and analyzed as part of an active surveillance program for bioterrorism might include the following:

- Number of patients seen in an Emergency Room
- Number of patients admitted to a hospital
- Number of EMS or ambulance runs performed each day, week, month, or other time period

Or

- Other data available from your facility that may indicate a change or trend in your community

preventing or reducing the morbidity and mortality, and the economic and social impact on the affected community following the attack. Mitigation is affected by national and international policies and the infrastructure of the public health system. A stronger public health infrastructure will ensure a more rapid and effective response, which in turn will decrease the negative impact of the event.

This leads us back into the preparedness phase of the emergency management model and completes a review of the flow of emergency management processes. Again, it should be emphasized that these are not processes that occur separate from each other; many phases overlap and occur simultaneously. It is also important for facilities and individuals to be constantly evaluating their disaster plans for gaps and educating staff members on their role in the plans.

So, how does an Infection Control Professional fit into this process? What is our role?

Certain aspects of bioterrorism preparedness, including self and facility assessment and development of a response plan, are responsibilities of the ICP. Other factions of bioterrorism preparedness may be filled by the ICP or they may be the responsibility of another qualified individual at your facility. For example, surveillance, whether active, passive or syndromic, would be the responsibility of the ICP or would at least be coordinated by the ICP.

Infection Control may spearhead other aspects of bioterrorism preparedness, such as the development of the facility bioterrorism response plan and facility assessment, or these duties could be assigned to Safety or the Environmental Health department at your facility. Tasks necessary for bioterrorism preparedness need to be discussed and assigned by the planning committee for your facility.

A healthcare facility's bioterrorism or disaster planning committee needs to be multidisciplinary and multi-agency. The ICP plays a critical role as a member of the planning committee, but their exact role may vary. In some facilities, the ICP may be the leader, coordinator or facilitator for the team. Each facility must assess the strengths of their own committee members and assign responsibilities accordingly.

Let's now switch to discussing bioterrorism preparedness as a whole and discuss the ICP's role in the process as it refers to the Preparedness and Response aspects of emergency management.

The first step in bioterrorism preparedness is to be aware of the risk. Following the September 11th attack on the World Trade Center and the Pentagon, the threat of terrorism has been at the forefront of American's minds. Prior to the fall of 2001, most Americans were not aware of the potential threat of terrorism. Despite this fact, terrorism has been on the rise in the past few years and there are more terrorist groups than ever before.

Since 1996, there have been an increasing number of threats of intended use of weapons of mass destruction, or WMDs. In 1996, the FBI tracked 37 incidents of WMD threats. In 2000, this number increased 7 fold to 257 threats.

In addition to the increase in number of WMD threats, the threatened method of attack has shifted. According to the FBI, the number of nuclear, chemical and biological WMD threats was approximately equal in 1997, but just one year later, biological agents had become the most frequently threatened method of attack. Bioterrorism accounted for more than half of the WMD threats in 1998.

In the fall of 2001, those threats became reality when anthrax was used as a bioterrorism agent in the form of letters mailed to media, news organizations and politicians. These letters emphasized the need for the US to be prepared for a bioterrorism attack. However, some communities still feel that they are not at risk.

As the memory of September 11th and the subsequent anthrax letters fade, many Americans are becoming complacent. The risk in complacency is that it deters us from our preparedness efforts. As Peter Sandman, a risk communications expert, has said, "denial masquerading as complacency is the biggest threat to preparedness."

Why is it important for ICP's, health care facilities and public health professionals to prepare for a potential bioterrorism attack?

Unlike traditional terrorism, healthcare and public health professionals will be the first responders in the event of a bioterrorism incident. With traditional terrorism you often have an explosion, a fire or smoke, some sign

how well educated the staff is prior to the incident. Just as nurses practice CPR on a regular basis so that the behavior becomes a natural response rather than something that feels uncomfortable, we also need to be familiar with disaster preparedness principles and plans and practice appropriate response behaviors.

The largest concern during the response phase will be patient management. What is your facility's surge capacity? How will your facility juggle a large number of acutely ill patients as well as deal with an influx of the worried well? Does your facility have the necessary equipment needed to meet the needs of the increase in patients? Are decontamination strategies and supplies available and is staff trained to perform this function? Where are you going to physically locate family members while patients are being triaged and treated? Most morgues can house fewer than a dozen bodies. How will your morgue handle a greater number of victims? Does your pharmacy have enough of the appropriate antibiotics on hand to dispense to employees, employees families, and victims until the National Pharmaceutical Stockpile or other resources become available? These are all questions that need to be addressed by your facility before a bioterrorism attack occurs.

Another important aspect of response is communication. Effective communication systems are essential to an effective response. You must be able to communicate both internally between departments and externally with outside agencies. In addition, communication with the general public in your community will be critical. During a crisis, the public will be looking for answers. Accurate, consistent messages must be provided as well as information regarding who is at risk and how those groups can quickly obtain treatment. Risk communication is one of the most challenging aspects of a response. Communication needs will be discussed in greater detail later in this presentation.

The recovery phase of the emergency management model consists of the interventions needed to return your facility and/or community to its pre-disaster baseline. This phase does not begin until the crisis is over. The goal is to return the community to normal functioning as soon as possible; including ensuring that healthcare and public health infrastructures remain intact. One of the largest components of the recovery phase is the replacement of lost resources. The response phase is resource-intensive and often leaves the facility or community depleted, in terms of physical and human resources as well as emotional and financial reserves.

You may need to restock personal protective equipment, medications and other medical supplies. You may also need to deal with a loss of staff that fell victim to the bioterrorism attack since healthcare workers often make up a large portion of a community's population. In addition to replacing lost resources, your facility or community will need to deal with the mental health and spiritual consequences of a bioterrorism attack. What we have learned from the World Trade Center and Pentagon attacks as well as other major terrorist incidents is that the consequences on mental health are great. Post Traumatic Stress Disorder, or PTSD, and related conditions, can quickly overwhelm a medical community.

Based on information from the Oklahoma City bombing, the New York State Office of Mental Health estimated that approximately 385,000 people living in the city of New York and another 38,000 that lived in suburbs of the city would suffer from some level of mental disorder following the September 11th attacks. These mental disorders range from mild feelings of depression or anxiety to PTSD requiring treatment. Furthermore, they estimated that approximately 2 million people living in the city and 1 million living in New York City suburbs would need crisis counseling for mental distress.

One of the unexpected findings was the increase in PTSD encountered in the first responders in New York; According to data released in May 2002, psychological symptoms persisted and were ongoing 6 months after exposure. In response, the New York State Office of Mental Health set up a 24-hour hotline for people to obtain free crisis counseling. This project, entitled Project Liberty, has received over 50,000 phone calls between September 11th and May 2002.

Following implementation of the plan and recovery, your organization or community needs to evaluate the process and identify gaps in the current plan. In addition, the process should be evaluated to determine better ways to mitigate the effects of a potential future incident. The preparedness plan should be updated based on these findings and these changes then need to be communicated to the participating groups in the form of education and planning exercises.

The last phase of the emergency management model, the mitigation phase, refers to sustained activities designed to prevent or minimize the negative impact of an event. In relation to bioterrorism, this refers to either

Transcript:
Role of the Infection Control Professional in Bioterrorism Preparedness

Hello and welcome to The Role of the Infection Control Professional in Bioterrorism Preparedness. My name is Terri Rebmann. I am the Infectious Disease Specialist at the Center for the Study of Bioterrorism and Emerging Infections at Saint Louis University, School of Public Health. In addition, I am certified in Infection Control. This presentation is meant to assist Infection Control Professionals in moving beyond acknowledging the risk of bioterrorism to preparing yourself and your facility to effectively respond to a bioterrorism attack.

As Infection Control Professionals (ICP), we play a vital role in maintaining the health of patients, visitors and employees in our facility as well as our community. We are experts in the fields of surveillance and epidemiology. In addition, it is imperative that we investigate outbreaks and initiate interventions to prevent the transmission of infections within the healthcare system. In order to be prepared for a bioterrorism attack, it is essential that we understand the epidemiology of bioterrorism and utilize our strengths to aid in the development and implementation of a bioterrorism response plan. We must educate ourselves on bioterrorism and commit to preparing our facilities and communities for the potential consequences following such an attack.

With the understanding of why we need to educate ourselves on bioterrorism, we now need to know where to begin. Although it presents some distinctive challenges, bioterrorism is similar to other emergency or mass casualty incidents and requires a similar response. A great place to begin, therefore, is with an understanding of the emergency management model.

This model was designed to display the process of community preparation for emergencies. It illustrates the processes of preparation, response, recovery, and mitigation. In addition, the emergency management model emphasizes evaluation and applying lessons learned to future events.

The emergency management model consists of four phases in a continuous process of activities. It is not designed to simply display a numbered sequence starting with preparedness and ending with mitigation, but rather it is a continuous cycle in which the phases overlap or sometimes occur simultaneously. However, for the purposes of this talk and ease of explanation, I will discuss each phase sequentially.

These phases include preparedness, response, recovery, and mitigation.

The preparedness phase involves all of the measures taken in preparing to handle an emergency, such as developing a plan, educating the work force, and conducting exercises. Education must be focused on all worker groups that will be involved in implementation of the plan. Training should include an overall description of the plan, participants' role in the plan, where and how to obtain resources, explanation of the communication system, and description of the reporting chain of command. This education needs to be a continual process, rather than a one-time event. Regular education updates are required to ensure staff comfort with emergency management processes and to alert staff to changes in the plan.

The next step in the emergency management model is the response phase. During the response, the plan you developed in the first step is implemented. The type of response necessary will depend on a number of factors, including the agent disseminated, the method of agent dissemination, the amount of agent released, how many people were exposed and how rapidly the event is identified.

For example, an incident involving one or more letters tainted with anthrax would require a different response than a covert release of aerosolized plague. This is because anthrax is not transmitted from person to person. Therefore, post-exposure prophylaxis for anthrax needs to be provided only to those exposed to the initial release. This would be very different for a *Yersinia pestis* release because pneumonic plague can be spread by respiratory droplets. Therefore, post-exposure prophylaxis for plague would need to be provided to those exposed to the initial release and close contacts of pneumonic plague patients.

The general principles, such as mass prophylaxis, are the same in both responses, but the scope of the response will be different.

The effectiveness of the response will depend a great deal on how well your plan is developed, to what extent your plan is integrated with other healthcare facilities and response organizations in your community, and