# WORKBOOK 5.1: GATHERING COMPONENT DATA

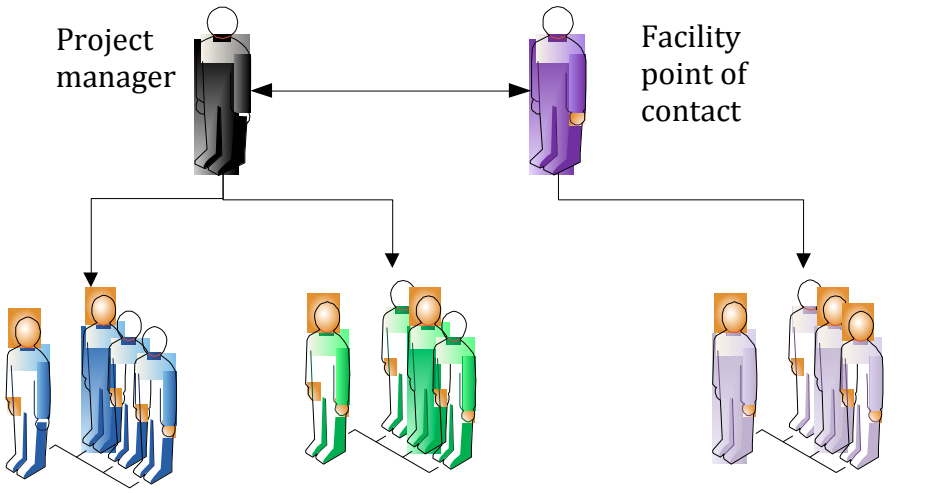
**Purpose** To provide information on gathering data on a critical infrastructure's functional components

## Vulnerability Analysis Team

A vulnerability analysis requires pre-execution planning, managing tasks during the project, and closing the project out with some type of report on the analysis.

A vulnerability analysis should begin with the formation of the vulnerability analysis team. Members of the team should include a project manager, who is responsible for coordinating and assigning tasks as required, and a security system technologist(s) who knows and understands the types of security countermeasures that could be installed at the site. This team should also include subject matter experts who understand the threat analysis process. Additional subject matter experts from the site, such as a safety expert, are required to ensure that all the critical assets are identified and their functional components analyzed appropriately. See Figure 1: Vulnerability Analysis Team.

**Figure 1: Vulnerability Analysis Team**




It is critical that subject matter experts from the selected facility be a part of the vulnerability analysis team. Such experts will provide accurate data about the site and specific operations, as well as expedite the team's ability to arrange site tours, identify individuals to be interviewed, and assist in completing the analysis.

Prior to arranging a site visit, the vulnerability analysis team project manager should request a data call, which simply means to request information about the site prior to actually performing the site visit. This call helps the subject matter experts and project manager determine the types of questions to ask while on-site and provides them with details on security systems and critical assets. The information to request regarding each component is listed in the checklists below. The data call is at least 30 days prior to the scheduled on-site visit to provide time for review of the data.

## Data Call Checklists

The data call checklists below help to make sure all considerations regarding the facility are discussed.

| **Physical Conditions** | |
|---|---|
| | Maps of the facility and topography |
| | Detailed site maps and drawings showing building locations and critical asset locations |
| | Interior facility drawings indicating critical asset locations and security system components, such as fences, alarms, and closed-circuit television cameras |
| | General information about climate and annual weather conditions |
| | Other (write below) |

| **Facility Operations** | |
|---|---|
| | Information that illustrates the facility's mission and critical assets |
| | Schedules of work activities to include open and closed periods involving critical assets |
| | Schedules of security force personnel to include numbers of personnel based on work schedules and shift changes |
| | Other (write below) |

| Facility Policies and Procedures as related to: | |
|---|---|
| | The security force, including standard operating procedures and protection strategies |
| | Access control and visitors |
| | Performance testing security measures |
| | Reporting unusual occurrences |
| | Protecting critical assets |
| | Past reports on violations related to facility security |
| | Protecting information technology |
| | Other (write below) |

| Regulatory Requirements | |
|---|---|
| | Regulations from the government authority responsible for the specific critical infrastructure |
| | Local emergency services response regulations |
| | Government mandated security regulations |
| | Past reports on regulation violations |
| | Other (write below) |

| Safety Considerations | |
|---|---|
| | Evacuation plans affecting critical asset area |
| | Emergency services response plans to critical asset areas |
| | Safety inspection reports concerning critical asset areas |
| | Other (write below) |

| Legal Considerations: Information concerning lawsuits that relate to: | |
|---|---|
| | Security force personnel, policy, and procedures |
| | Searching of employees and visitors to the facility |
| | Failure to provide proper training issues |
| | Failure to comply with regulatory requirements |
| | Any information on the final outcome of such legal issues |
| | Other (write below) |

Once the data call is initiated, arrangements for the site visit are made with the primary point of contact for the critical infrastructure site. Ideally, it is this individual's responsibility to arrange interviews with site experts and conduct tours as necessary.

### Data Review Questions

Examples of potential questions for each component are listed below. Actual questions will depend on the site and the information reviewed from the data call.

### Physical Conditions

1. Has any building on the facility been threatened by a natural disaster or terrorist attack?
2. Has the topography or vegetation in the area prevented the security systems from working as they should?
3. Does the location of the facility allow easy access to outsiders such as the public?
4. Is the facility layout as depicted in the maps and drawings still accurate?
5. Are structures on the site still depicted accurately on the facility drawings?
6. Are infrastructure details such as ventilation and air conditioning, communications and information systems, location of hazardous materials available for review?

### Facility Operations

1. What is the mission of the facility and how does the critical infrastructure contribute to the mission?
2. Does the schedule of work activities reflect what was received during the data call?
3. Does the security force know and understand their guiding policies and procedures?
4. What is the work schedule of those involved with the facility operation? Your response should include open and closed periods, weekends, and holidays.
5. What are the security clearance requirements of employees? What are their respective job descriptions?
6. Are visitors allowed in the facility and if so, how is access controlled?

## Facility Policies and Procedures

1. What are the security requirements for security force personnel at the facility?
2. When was the last time, the security force conducted a performance test. If conducted, what were the results?
3. Can you show me the reports on violations of policies and procedures?
4. Are security systems performance tested, if so, when was the last test and what were the results?
5. Are the security systems performing as designed? As an example, do the sensors operate properly, does the closed circuit television view truly indicate who or what is in a specified area, and lastly are the physical barriers to the facility adequate?

## Regulatory Requirements

1. Who is the regulating authority for this facility, and is there more than one?
2. When was the last regulatory audit? What were the results?
3. What has the facility done to comply with regulations and findings by the authority?
4. Are there regulatory requirements for the facility's security force?

## Safety Considerations

1. When was the last safety inspection conducted of the facility area(s)?
2. Does the inspection include life safety issues such as confined space reviews (ensuring people are able to safely work in and escape from spaces that have limited access)?
3. Who responds to emergency situations such as fire and medical issues?
4. When was the emergency response plan last tested? What were the results?
5. Is there an evacuation plan? Has the plan been exercised?

## Legal Considerations

1. Are there any legal constraints on the facility and how it operates? If so, what are they and how do they affect security operations?
2. Are there any current legal issues at the facility? If so, what are they?
3. What are the legal regulations that govern the security force's actions against a terrorist?
4. What are the past legal issues affecting the facility's operations?

This previous list of questions illustrates the types of questions you will be asking during an interview. Additional questions will be provided for you as you progress through the material in each module.

This Page Intentionally Left Blank.