

NORTH CAROLINA DEPARTMENT OF AGRICULTURE
&
CONSUMER SERVICES

Terrorism Threat Vulnerability Self Assessment Tool

Dear Industry Partner,

The Terrorism Threat Vulnerability Self Assessment tool is a guide to help you better understand your potential vulnerabilities to terrorism. The conduct of a vulnerability self assessment is voluntary for the North Carolina agri-business community but you are strongly encouraged to perform this self assessment for each of your organization's facilities. A facility is any administrative, industrial activity or laboratory complex where departmental employees perform their duties in office, warehouse, industrial or laboratory space.

This tool is not intended to replace any current reporting requirements, such as those for hazardous materials or other emergency events. This vulnerability assessment tool is intended to assist managers with determining what vulnerabilities may exist within their organizations that might increase their exposure to a terrorist event and to assist your organization, and local law enforcement, in assessing your overall vulnerability to such an event. While no steps can provide absolute protection, experience has shown that adoption of heightened awareness, basic defensive steps, increased monitoring or correction of vulnerabilities and close coordination with local law enforcement will reduce the likelihood of a terrorist act. This self assessment can be accomplished with little or no cost in a fairly short period of time. Guidance on how to complete the self assessment is included with the Self Assessment Tool.

Threat vulnerability self assessments prepared by your organization should be provided to local law enforcement agencies who have primary first responder responsibility to the location of your business activity or organization whenever the assessed vulnerability score is determined to be "High Risk" or if there is deemed to be any significant or dangerous factors that should be brought to the attention of law enforcement. The completed Self Assessments should be submitted by hand or US MAIL, in digital form or hard copy. It is recommended that you do not send it by Email.

The Terrorism Threat Vulnerability Assessment should also be conducted at least annually and anytime there is an increased threat of a terrorist event and whenever there is a significant change to your organization's facilities or activities. The completed Vulnerability Self Assessment is a confidential law enforcement tool which should be used by your organization and local law enforcement to assist in preventing criminal acts committed by terrorists and it is exempted from disclosure under the Public Records Law by General Statute 132-1.4.

North Carolina Department of Agriculture and Consumer Services

TERRORISM VULNERABILITY SELF-ASSESSMENT

This vulnerability self-assessment is intended to assist your organization to determine if it is vulnerable to terrorism and to assist you and law enforcement in assessing the overall vulnerability of your organization. It provides guidelines for conducting a vulnerability self-assessment. It can, and should be, customized, where appropriate, to your specific facilities activities. This is intended to be a general tool for general use. It may not include all issues that would be considered in your specific situation. Therefore, it is imperative that you consider the unique character of your organization: its functions, its general public image, its overall public visibility. Consider both **who** may work in your organization and **what** your organization does. Assess the symbolic value of your organization to the public or within your own industry. This assessment does not replace any current reporting requirements.

Some organizations or activities may not present a likely target for terrorism. Others' activities may make them a more likely terrorist target. This is a subjective process and will be determined by the nature of the terrorist threat at any given time and by input from local law enforcement's assessment of the threat in your area. Remember, you must consider all potential terrorism threats, both domestic and international. The score you assign in each subject area is based on your judgment of your organization's posture in that subject area measured on a scale from low to high vulnerability. The evaluation covers a broad range of topics and is not based merely upon the fact that your organization may house hazardous materials, conduct what some groups may consider controversial activities or perform important public/industry functions. Your organization's self-assessment of vulnerability, the level of threat in your area and available resources will determine the level of threat reduction measures that your organization should consider implementing.

It is important to remember that the most important threat reduction measure is vigilance on the part of your organization's staff, their awareness of anything out of the ordinary and their prompt communication of that information to your organization's security team or management.

Vulnerability Self-assessments completed by or provided to State or local governments will be used to prevent crime and are exempt from disclosure under the Public Records Law under G.S. 132-1.4. Threat Vulnerability Self-Assessments in the possession of private organizations are not Public Records. Completed Terrorism Vulnerability Self-Assessments should be provided to local law enforcement in hard copy or on digital media. They should not be e-mailed.

The Vulnerability Self-Assessment should be conducted at least annually and any time there is an increased threat of a terrorist event or whenever there is a significant change to your organization's facilities or activities.

Name of Agency/Business: _____

Mailing Address: _____

Location: _____ **Date:** _____

Note: Please provide the Latitude, Longitude and elevation of the main entrance to your facility. If you do not have access to a GPS unit, please contact your local law enforcement office for assistance.

Circle on each scale your evaluated score. Then total the scores and enter the total on the last page.

1. Potential Terrorist Intentions

Low Vulnerability	High Vulnerability
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	

Issues to be considered in selecting your score:

- ? Are you aware of any terrorist threat to your organization?
- ? Are you aware of a history of terrorist activity in your area or your specialty?
- ? Are you aware of the level of capability of any suspected terrorist which you believe poses a threat to your organization?

2. Specific Targeting

Low Vulnerability	High Vulnerability
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	

Issues to be considered in selecting your score:

- ? Have you obtained current information from law enforcement or other sources that your organization has been targeted by terrorists?
- ? What is the reliability of these information sources?
- ? What is your organization's public visibility?
- ? Does the nature of your organization's activity lead you to think it may be targeted?
- ? Are there activities that indicate possible terrorist preparations in your area or specialty?

3. Visibility of your Facility/Activity within the Community

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score

- ? Is your organization well known in the community?
- ? Do you regularly receive media attention?
- ? Is your organization nationally prominent in your field or industry?
- ? Is your location and the nature of your activity known generally to the public?

4. On-Site Hazards

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Are hazardous materials, explosives or other dangerous items on your site?
- ? Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?
- ? Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?
- ? Can any products stored or used on your site be used as or in the manufacture of a mass casualty weapon?
- ? Can any products stored or used on your site cause extensive environmental damage?

5. Population of Site/Facility/Activity

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have more than 250 people normally present at your site?
- ? Do you have more than 1,000 people normally present at your site?
- ? Do you have more than 5,000 people normally present at your site?
- ? Do you hold events at your site that attracts large crowds?

6. Potential for Mass Casualties

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do the materials stored or used at your site have the potential to create mass casualties on-site?
- ? Do the materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
- ? How many people live or work within one mile of your site: 500; 1,000; 2,000; 5,000; more than 5,000?

7. Security Environment & Overall Vulnerability to Attack

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Does your organization have effective internal security procedures?
- ? What is the law enforcement presence in your area?
- ? What is the hardness, level of blast protection, etc. of your facilities?
- ? How accessible (security presence, access control, ID badges, metal detection, buffer zones, fences, etc.) of your facility?
- ? Are your assets and/or its potential recognized as a symbol?
- ? What level of public access is necessary for you to function?
- ? Can you control high-speed vehicle approaches to your facility?
- ? Do you have access control to your parking area?
- ? Do you conduct vehicle searches when entering facility grounds or parking areas?
- ? Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc)?
- ? Is parking permitted adjacent to or near your buildings?
- ? Is your delivery area supervised during hours of normal business?
- ? Is your delivery area access blocked during hours that your business is closed?

8. How Critical are your Products or Services ?

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? What is the importance of your organization to the community?
- ? What is the importance of your organization to your industry?
- ? Is your organization critical to the local population, economy or government?
- ? Is your organization critical to the continuity of basic services or utilities infrastructure in your area?
- ? Is your organization critical to state or national commerce?
- ? What would be the effects of a terrorist act against your organization?
- ? What would be the social, economic or psychological ramifications of a terrorist attack against your organization?
- ? What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc?
- ? How long would it take to restore your critical services/functions?

9. High Risk Personnel

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have personnel that are critical to the continuing function of State or local government, basic services, utilities infrastructure, the community, the economy, and/or are of inherent value to your business or agency?
- ? Do you have personnel that are critical for responding to a terrorist act?
- ? What would be the effect of a terrorist act against these high risk personnel?

10. Organization Communications

Low Vulnerability	High Vulnerability
1	20

Issues to be considered in selecting your score:

- ? Do you have a Mass Notification System (public address system, intercoms, alarms)?
- ? Do you have a secure communications network that can be relied upon during a crisis?
- ? Do you have a crises response team?
- ? Is your crisis response team trained?
- ? Do you conduct regular exercises?
- ? Do local/regional emergency responders participate in your exercises?
- ? Does your Crisis Response Team have its own portable communications system?
- ? Can your Crisis Response Team communicate directly with emergency responders?
- ? Do you have an emergency law enforcement notification system such as a hot line, panic button or something similar?
- ? Is your alarm system tied into the local law enforcement department or do you have an alarm service?
- ? Are your systems tested regularly?

11. Security and Response

Low Vulnerability	High Vulnerability
1	20

Issues to be considered in selecting your score:

- ? Are your security forces staffing and training levels adequate?
- ? Do you have the capability to maintain a security presence in a high threat/situation?
- ? Are additional security personnel available if requested?
- ? Are there affiliated agency/industry/organization support services available?
- ? Do you have trained disaster response teams within the organization?
- ? Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?

- ? Are local/regional law enforcement forces adequate and can they respond rapidly?
- ? Are local emergency responders familiar with your facility and its contents?

12. Policy/Procedures/Plans

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have a current crisis response/disaster plan?
- ? Does your plan include the types of crisis you are most likely to encounter (e.g., fire, explosion, chemical release)?
- ? Are your employees familiar with the plan?
- ? Have you conducted crisis response and disaster drills and were they effective?
- ? Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

13. Security Equipment

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have a security system and is it current technology?
- ? Do you have an intrusion monitoring motion detector or an alarm system.
- ? Do your systems have back-up if power is cut or fails?
- ? Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?
- ? Is such equipment in working order and has it been inspected recently?

14. Computer Security - Cyber-Crime & Cyber-Terrorism

Low Vulnerability	High Vulnerability
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	

Cyber-crime, including cyber-terrorism, involves attacks against your organization's computers systems and your data.

Issues to be considered in selecting your score:

- ? Is your site dependent on information technology such as computers and networks to accomplish its daily business activities?
- ? Is the information stored in your computer systems valuable?
- ? Do you have back-up power available for your computer systems?
- ? Do you make back-up copies of your data?
- ? Is your back-up data securely stored?
- ? Does your site have computers or networks connected to the Internet?
- ? Have you experienced problems with computer security incidents, such as computer viruses, worms, web-site defacements and/or denial of service attacks in the past?
- ? Do you have staff who are adequately trained and are available to monitor security warnings and take protective measures, such as loading system patches?
- ? Do you have technology security tools in place such as firewalls, intrusion detection systems or anti-virus software to protect your computer systems?
- ? Do you have a computer security policy, plan and procedure in place that includes a computer security incident response team?

15. Suspicious Mail And/Or Packages

Low Vulnerability	High Vulnerability
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	

Issues to be considered in selecting your score:

- ? Is the mail for your facility opened in a secured area or an area isolated away from the majority of personnel?
- ? Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?

- ? Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
- ? Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

16. Telephone Bomb And Other Threats

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Has your staff received training on how to handle bomb and other threat calls?
- ? Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
- ? Does your facility have a plan on how to handle bomb and other threatening calls?
- ? Does your plan include a system for searching your facility for suspicious objects, which would be done by qualified personnel familiar with the facility?
- ? Does your plan include a decision making process on whether to evacuate the facility ?
- ? Are personnel familiar with the plan and have evacuation drills been conducted?
- ? Is your plan coordinated with local law enforcement and the local phone company?

17. Employee Health & the Potential for Bio-Terrorism

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have an employee occupational health specialist on staff?
- ? Do you have an occupational health safety program in place?
- ? Do you have a health professional working at your facility?
- ? Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?
- ? Do you monitor the health status of employees on sick status or absenteeism?

- ? Are employees encouraged to keep supervisors informed on any unusual health related event or condition?
- ? Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, such as strange substances or odors from packaging or mail?
- ? Do employees know the proper procedures for emergency operation or shut-off of air handler, air circulating or ventilation systems?
- ? Do you keep a current list of employees, home addresses and emergency contact information?
- ? Do you have an emergency notification plan for employees (e.g. calling tree)?

Note: Items 18 & 19 are to be completed by Health Care Activities / Organizations Only.

18. Capacity to Recognize a Bio-Terrorism Event

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you regularly notify the state or local health department of all reportable diseases and conditions when they occur in your facility?
- ? Do you have personnel trained in recognizing the clinical signs and symptoms of potential victims of biologic or chemical events?
- ? Do you have a plan for responding to suspected Bio-Terrorism events?
- ? Do you regularly communicate unusual symptoms or patterns of disease with other healthcare facilities in your area or the local health department?

19. Capacity to Respond to a Bio-Terrorism Event

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ? Do you have a Bio-Terrorism response plan for your facility?
- ? Have you coordinated your Bio-Terrorism response plan with the local emergency operations team including law enforcement and other healthcare facilities?
- ? Do you have a system for knowing the bed (or care) capacity of your facility at any given time?
- ? Do you have a current inventory of your medical supplies and pharmaceuticals that may be required during an emergency event?
- ? Do you have a plan for contacting and deploying healthcare personnel during an emergency?
- ? Do you have plans for how to best utilize your facility during a mass casualty event?
- ? Do you have decontamination facilities?
- ? Do you have a protocol for treating contaminated patients?
- ? Do you have a plan for how to utilize volunteers from other areas and facilities during an emergency? (e.g. Scheduling, Training, Credentialing, etc.)

Remarks/Unusual or Significant Issues:

Please list any important remarks you think should be made concerning your self-assessment. Also, please list any unusual or significant findings that you developed during your self-assessment, list significant hazardous materials that might be used as a terrorist weapon or any significant impact a terrorist act against your site may cause to the community.

Attach an additional sheet if necessary.

Group Performing Self-Assessment:

Type of Business/Facility: _____

Contact Person: _____

Address: _____

Phone No: _____

Fax No: _____

E-Mail Address: _____

(For information sharing ONLY)

Who is Your Local Law Enforcement Contact?

You should coordinate with your local law enforcement agency regarding the results of your self-assessment. If your self-assessment indicates that your score is in the High Risk category, or if you believe your organization presents significant or unusual vulnerability or risk factors, you should provide a copy of this self-assessment to your local law enforcement office.

Total Score: _____

Self-Assessment Evaluation:

(Please note that if the two health organization questions are completed, you will need to adjust the following scoring bracket ranges to increase the potential total score to 380)

Low Risk	Below 85
----------	----------

86	Low Caution	170
----	-------------	-----

171	High Caution	255
-----	--------------	-----

256	High Risk	340
-----	-----------	-----