The Librarian's Disaster Planning and Community Resiliency Workbook

Librarians Fulfilling Their Role as Information First Responders

PRESENTED BY THE

NJ State Library
An affiliate of Thomas Edison State University

PO BOX 520 | 185 WEST STATE STREET | TRENTON NJ 08625

www.njstatelib.org

FUNDED BY A GRANT FROM THE

PSEG Foundation

Table of Contents

Section A-1: Emergency Action Plan 3
Suggested Table of Contents 4
Time of Event 4
Library Location and Identification Information 4
Reporting Emergencies 5
Evacuate Notice 5
Move to a Central Shelter Notice 5
Shelter–In-Place Notice 5
All-Clear Notice 6
Damage Assessment Team 6
Notification Signals for People with Disabilities 6
Crisis Communication Plan 6
Communicating with Management during a Crisis 6
Essential Staff Contact Information 6
Public Notice of Emergency Conditions 7
Shutdown of Critical Systems 7
Securing Collections and Other Assets 7
For Events with a Lead Time of Greater Than <X> Hours. 7
For Events with a Less Then <X> Hours 8
For No-Notice Events. 8
Accounting for Personnel 8
Appendix A: Facility Floor Plan 8
Facility Floor Plan 9
Appendix B: Emergency Contact List 10
Section A-2: Disaster Recovery Plan 11
Suggested Table of Contents 12
DRP General Policies and Procedures 12
Emergency Services 13
List of Pre-Approved Vendors 13
Emergency Shutdown and Restart Procedures 13

Inventory of IT equipment 15
Examples 15
Staff IT Equipment 15
Public Use IT Equipment 16
Inventory of Office Equipment 16
Second Floor Offices 16
Inventory of Public Use Office Equipment 16
Inventory of Security Equipment 17
Standby Power Generator 17
Appendix A- Library Power Diagram 18
Appendix B – Plumbing Diagram 19
Section A-3: Continuity of Operations Plan 20
COOP Background and Authority 21
Household and Family Preparedness Planning 21
Section A-4: Community Reengagement Plan 22
Checklist of Community Resiliency Services 23
Onsite Services 23
Outreach Services 23
Section B: Additional Worksheets 24
General Security Checklist 24
Dealing with Disruptive People Checklist 25
Warning Signals: Trust Your Instincts 25
Be Aware of Your Surrounds 25
Try to Defuse the Situation 25
What to do if They Won't Leave? 26
What to Avoid 26
If in a Crowd 27
Summary Comments 27
Risk Assessment Worksheet 28
Risk Matrix 29
Section C: List of Identified Hazards by State 30
Section E: Glossary of Cyber-Security Terms 44

Section A-1: EAP

Emergency Action Plan (Template)

Last Updated: (DD/MM/YYYY)

(Insert library Logo)

(Street Address)
(City, State, Zip Code)
(GPS Coordinates)
(Telephone)

Suggested Table of Contents

- Time of Event
- Library Location and Identification Information
- Reporting Emergencies
- Evacuation Notice
- Move to a Central Shelter Notice
- Shelter in Place Notice
- All-Clear Notice
- Notification Signals for People with Disabilities
- Crisis Communication Plan
- Communicating with Management During a Crisis
- Essential Staff Contact Information
- Public Notice of Emergency Conditions
- Shutdown of Critical Systems
- Securing of Collections and Other Assets
- Accounting for Personnel
- Appendix A: Facility Floor Plan
- Appendix B: Extended Contact List

Time of Event

The following incident was reported to library staff:

- <Type of Event>
- <Time of First Report>
- <Name of person Making the Initial Report>
- <Time of First Response>

Library Location and Identification Information

Please complete the following for each facility covered by this Emergency Action Plan (EAP). **NOTE**: Consider including GPS coordinates in this section of the plan since in the aftermath of a severe storm or other devastating event, street signs and normal addresses may not be available or reliable.

Location Information

Official Name of the Organization: _____
Primary/Main Entrance Address: _____
_____
GPS Coordinates: _____
Primary Telephone Number: _____
Name of Emergency Contact: _____
Telephone/ Cell Phone: _____
Email Address: _____
Alternative Emergency Contact: _____

Telephone/Cell Phone: _____
Email Address: _____

Reporting Emergencies

In the event of a significant emergency, staff should immediately call 911. A second notification will be given to Emergency Response Team (ERT) who will take additional steps to assist in responding to the emergency such as activating the fire alarm. To contact the ERT <insert notification process>.

Evacuate Notice

In the event that an evacuation is required, the following signal will be used.

- Audio Signal: <insert alarm signal such as "one long continuous horn sound," etc.>
- Visual Signal: <insert alarm signal such as "flashing white strobe light in each corner of the building," etc.>
- Additional Notification: <insert instructions such as "Safety Wardens take their stations and begin directing traffic flow to designated area and will render assistance to any people with disabilities who need help in evacuating.">

Once you become aware of the evacuation signal, move immediately to leave the building following the predetermined evacuation route. Those assigned safety tasks, should move to their assigned areas if safe and practical to do so.

Move to a Central Shelter Notice

In case of a release of hazardous material or a severe weather situation such as a tornado, the following signals will be used.

- Audio Signal: <insert alarm signal such as "one short intermittent horn sound," etc.>
- Visual Signal: <insert alarm signal such as "flashing red light visible throughout the building," etc.>
- Additional Notification: <insert instructions such as "Safety Wardens take their stations and begin direction traffic flow to designated area and will render assistance to any people with disabilities who need help in reaching the shelter.">

Once you become aware of this signal, move immediately to the central shelter following a predesigned route. Those assigned safety tasks should move to their assigned area if safe and practical to do so.

Shelter–In-Place Notice

In certain emergencies such as workplace violence there may not be time to move to a central shelter. In these situations, individuals must make their own decision to *run, hide* or *fight*. If you decide to stay in your work area, find a secure hiding spot that provides some protection and keeps you out of sight. If safe to do so, remain there until the All Clear signal is sounded or you are contacted by First Responders, such as the police.

Those assigned safety tasks should move to their assigned areas unless otherwise directed. The alarm for this scenario is:

- Audio Signal: <insert alarm to be used>
- Visual Signal: <insert alarm to be used>
- Additional Notification: <insert other means of communications, such as text messaging>

All-Clear Notice

At the end of the emergency, an "*All Clear*" notice will be issued by the Emergency Response Team. This notification may be verbal, via email/social media or an audible/flashing light signal that indicates it is safe to return to the work area and resume operations.

If the emergency lasts for a prolonged period, arrangements will be made to contact staff who have left the immediate area.

Damage Assessment Team

Once the All Clear signal is given and before the staff is allowed back into the facility, a pre-designated team will enter the building and inspect for damage. These individuals will be chosen for their knowledge of the facility and associated infrastructure and will document any signs of damage. They will also secure certain areas if they deem it inappropriate or dangerous for others to enter part of the facility. The members of this team are:

- <Name> <Responsibility> <Contact Info>
- <Name> <Responsibility> <Contact Info>
- <Name> <Responsibility> <Contact Info>

Notification Signals for People with Disabilities

All emergency alerts and notifications will take into account the needs of individuals with disabilities. Appropriate equipment such as stair chairs and other useful tools will be stored in an easy to access area for use during an evacuation or sheltering emergency.

Be sure to have an evacuation plan which takes into account the challenges faced by anyone with a disability. This includes having easy and quick access to special equipment (e.g. a "stair chair" for those who cannot negotiate stairs). This requirement extends to any staff member who is temporarily injured and unable to move well or respond to various evacuation/sheltering orders. Pay special attention to this issue since it is a legal requirement placed on all employers or those operating a place of business.

Crisis Communication Plan

A list of critical support staff along with their contact information can be found (insert location such as "see Appendix B").

Communicating with Management during a Crisis

When an emergency occurs the following procedures are to be followed:

- <Designate who is responsible for these actions.>
- <Indicate who is to be contacted, in what order, and the primary and secondary ways (more if possible) they should be contacted. Will this procedure be different if the event occurs during the day, during the evening, or outside normal working hours?>

Essential Staff Contact Information

In the event of an emergency, at a minimum, the following roles will be immediately activated:

- Incident Commander. <Include information on how to determine who the correct incident commander is.>
- <Include here the names of anyone else you feel should be contacted in the initial stages of a crisis. For example, the mayor's office or State Library.>
- If the Incident Commander determines that more support is needed, he/she will follow the following protocol for activating other members of the response team and/or ordering a general evacuation/or sheltering to take place.>

Public Notice of Emergency Conditions

- Once the incident commander has made a determination as to the seriousness of the event and appropriate management and staff have been contacted, the following procedure will be followed to inform the public of the situation and update them on any change to the library's operating times and list of available services. <Insert procedure including how and when to contact mass media outlets such as local TV and radio. Also describe the appropriate use of social media to spread word of the changes.>

Shutdown of Critical Systems

Before leaving the facility or moving to a sheltered location, those charged with the shutdown of critical operations should (insert instructions such as "complete their assignment and then move to safety, if this is practical").

Securing Collections and Other Assets

As caretakers of the public's assets, it is the responsibility of the library staff to ensure the protection and security of items and collections entrusted to us.

If an emergency occurs that requires an evacuation of the library, the following procedures will be followed:

For Events with a Lead Time of Greater Than <X> Hours.

Given sufficient notice, the following items will be packed in suitable containers and evacuated from the library:

- <Give list of items to be moved as well as their location. Include any special handling conditions such as "Do not touch first editions with bare hands." or "Do not expose the art collection to direct sunlight.">
- <Designate who is responsible for these actions.>
- <Packing material and suitable containers are stored <insert location or directions on how to obtain same, such as "Go to a local craft store and purchase 5 large plastic containers with secure lids.">
- Any other special directions including how to inventory the items, where to send the inventory, information, and instructions on security the material. If useful, suggest taking photos of the items being packed and include these in with any shipping invoices or records.

For Events with a Less Then <X> Hours.

For short notice events threatening the library, take the following steps:

- <Give list of items to be secured as well as their location. Include any special handling conditions such as "Do not touch first editions with bare hands." or "Do not expose the art collection to direct sunlight.">
- <Designate who is responsible for these actions.>
- <If the material is to be secured in a special way, indicate this information here>
- Any other special directions including how to inventory the items and where to send the inventory information. If useful, suggest taking photos of the items being packed.

For No-Notice Events.

- Describe the actions to be taken in the event of an emergency that arises without warning. Be sure to designate who is responsible for these actions and empower them to ignore these instructions if they do not feel safe in carrying them out.

Include any supplementary information related to the protection of collections, artifacts and other assets here.

Accounting for Personnel

Once at the assembly or shelter site, the person in charge must attempt to account for the location of everyone who is at the facility. As Safety Wardens arrive, they should report on the status of their area. This includes verifying that everyone has left their assigned area and no one remains in that part of the facility.

The individual in charge of the assembly area or shelter should be prepared to brief the arriving First Responders on the nature of the emergency and provide an accurate accounting for all staff and visitors.

Appendix A: Facility Floor Plan

A current floor plan of the facility can be found (insert location such as "in the Appendix A section of this plan"). Designated members of the emergency response team have a responsibility to shut down operations of critical services in the event of an order to evacuate the building or move to a sheltered location. Key among these responsibilities is checking to determine if the correct shutoff values have been closed. The location of all shutoff switches and emergency stop buttons are listed on this floor plan.

An up-to-date list of the type, quantity and location of any hazardous or explosive materials stored onsite is also noted on the floor plan in (insert location such as "in the Appendix C section of this plan").

All exits are periodically inspected and found to be accessible as of the date of this plan.

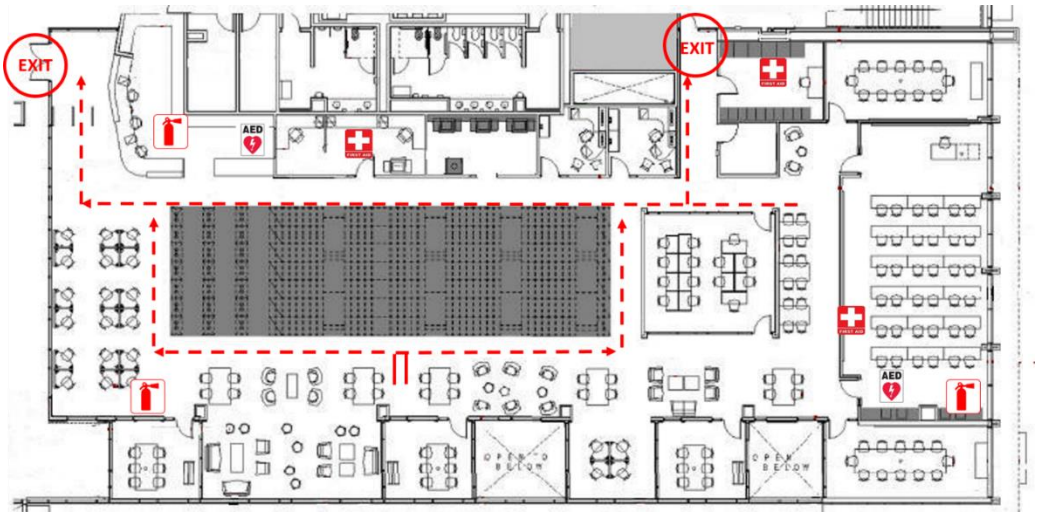
All locks have been inspected and judged to be in good working order.

Fences or other perimeter enclosures have been inspected and found to be in good working order as of the date of this plan.

All monitoring devices, closed circuit television cameras, security lights, and other security devices are periodically inspected and have been judged to be in good working order as of the date of this plan.

Facility Floor Plan

The following is a sample floor plan showing an escape route and placement of some emergency equipment.



LEGEND

- Automatic External Defibrillator:

1st Aid Kit:

Fire Extinguisher:

Appendix B: Emergency Contact List

Modify as required. Insert actual names where possible – (example: The Good Coverage Insurance Agency)

Police Department	(XXX-XXX-XXXX)	
Fire Department	(XXX-XXX-XXXX)	
<Local Ambulance Service>	(XXX-XXX-XXXX	
American Association of Poison Control Centers	(800-222-1222)	
Emergency Message Line	(XXX-XXX-XXXX)	
<Alarm Company>	(XXX-XXX-XXXX)	(Contact Person)
<Facilities and Groundkeeper>	(XXX-XXX-XXXX)	(Contact Person)
<Local Ambulance Service>	(XXX-XXX-XXXX)	
<Insurance Agency>	(XXX-XXX-XXXX)	(Contact Person)
Policy #:		
<Local Electric Power Company>	(XXX-XXX-XXXX)	
<Gas Company>	(XXX-XXX-XXXX)	
<Telephone Company>	(XXX-XXX-XXXX)	
<Waste Disposal Service>	(XXX-XXX-XXXX)	
<Plumber>	(XXX-XXX-XXXX)	(Contact Person)
<Electrician>	(XXX-XXX-XXXX)	(Contact Person)
Public Works	(XXX-XXX-XXXX)	
<Local TV>	(XXX-XXX-XXXX)	
<Local Radio>	(XXX-XXX-XXXX)	
<Information Technology Team>	(XXX-XXX-XXXX)	(Contact Person)
<State Facility>	(XXX-XXX-XXXX)	(Contact Person)
<Preservation and Archive Services>	(XXX-XXX-XXXX)	
<Other>	(XXX-XXX-XXXX)	

Section A-2: Disaster Recovery Plan

Disaster Recovery Plan (Template)

Last Updated: (DD/MM/YYYY)

(Insert library Logo)

(Street Address)
(City, State, Zip Code)
(GPS Coordinates)
(Telephone)

Suggested Table of Contents

- DRP General Policies and Procedures
- List of Pre-approved Vendors
- Emergency Services
- Emergency Shutdown/Restart Procedures
- Inventory of IT equipment
    - Staff Equipment
    - Public Use Equipment
- Inventory of Office Equipment
    - Location of Manuals
- Inventory of Public Use Equipment
    - Location of Manuals
- Inventory of Security Equipment
    - Location of Manuals
- Software License Inventory
- Standby Power Generator
- Calendar of Upcoming Staff Training Classes
- Appendix A: Library Electrical Diagram
- Appendix B: Library Plumbing Diagram

DRP General Policies and Procedures

File Backups: It is the policy of the <NAME> Library that all online files designated as critical will be backed up <frequency, example – weekly> via <describe mechanism, for example "writing the files to a DVD">

These backup files will be <describe how the files will be handled, how they will be labeled for identification (date of backup?), and sent to an offsite location. Then name the vendor, their location and contact information>

If a file needs to be retrieved <describe the procedure. For example, "An authorized staff member will call and arrange for the specific file to be sent to the library the next day." See form below.>

Weekly Backup Procedures ***<Library Name>***

Date: _____ Volume Identifier: _____

Contents: <For example: Weekly timecards and expense reports>_____

Sent to: <Vendor Name> <Vendor Address>_____ <Phone Number>

To Retrieve Any File Contact: <Name>_____ <Method of Contact (Phone or email)>

Other Comments: _____

_____

_____

Emergency Services

If the facility or any equipment sustains damage, it is the policy of the library that the Head Librarian can authorize on-the-spot repairs up to <$X,XXX>. Every effort should be made to have these repairs made during normal working hours to reduce overtime charges. A list of approved vendors follows.

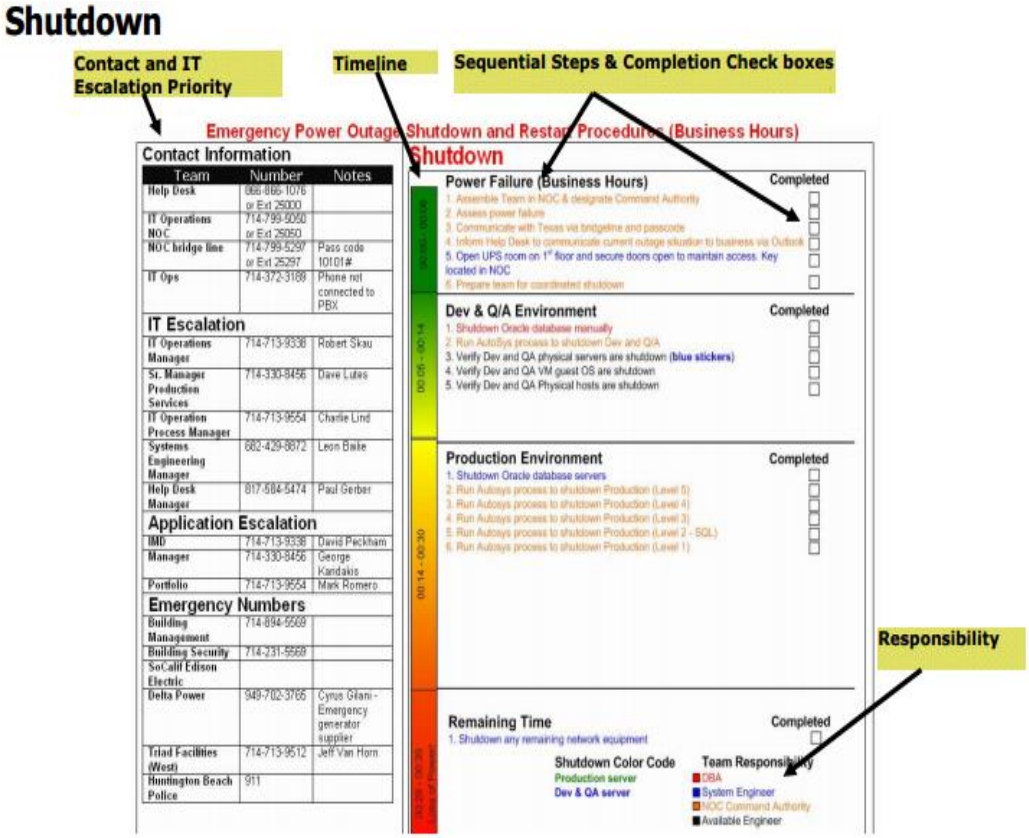
List of Pre-Approved Vendors

Modify as required. Insert actual names where possible – example, *Good Hands Plumbing*)

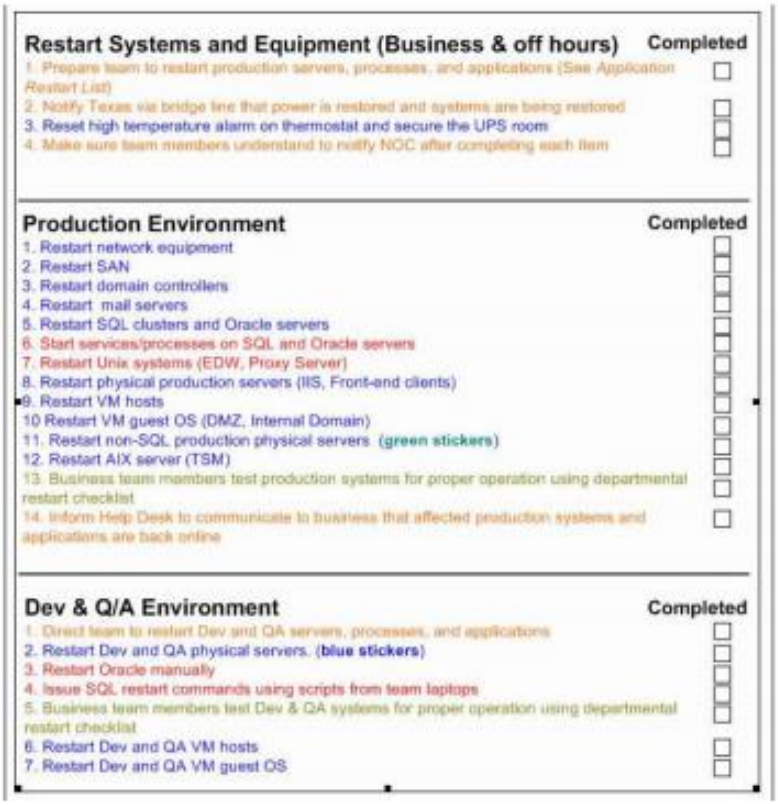
Electrical Work	(XXX-XXX-XXXX)	Contract ID # (34-1256689)
IT Support	(XXX-XXX-XXXX)	Contract ID # (97-1668689)
Plumbing Work	(XXX-XXX-XXXX)	Contract ID # (21-1333869)
Landscaping/Debris Removal	(XXX-XXX-XXXX)	Contract ID # (47-1009689)
<OTHER>	(XXX-XXX-XXXX)	Contract ID # (16-3690011)

Emergency Shutdown and Restart Procedures

When shutting down IT equipment, use the following procedures.



When restarting IT equipment, use the following procedures.



Restart Systems and Equipment (Business & off hours) — Completed

1. Prepare team to restart production servers, processes, and applications (See Application Restart List)
2. Notify Texas via bridge line that power is restored and systems are being restored
3. Reset high temperature alarm on thermostat and secure the UPS room
4. Make sure team members understand to notify NOC after completing each item

Production Environment — Completed

1. Restart network equipment
2. Restart SAN
3. Restart domain controllers
4. Restart mail servers
5. Restart SQL clusters and Oracle servers
6. Start services/processes on SQL and Oracle servers
7. Restart Unix systems (EDW, Proxy Server)
8. Restart physical production servers (IIS, Front-end clients)
9. Restart VM hosts
10. Restart VM guest OS (DMZ, Internal Domain)
11. Restart non-SQL production physical servers (**green stickers**)
12. Restart AIX server (TSM)
13. Business team members test production systems for proper operation using departmental restart checklist
14. Inform Help Desk to communicate to business that affected production systems and applications are back online

Dev & Q/A Environment — Completed

1. Direct team to restart Dev and QA servers, processes, and applications
2. Restart Dev and QA physical servers. (**blue stickers**)
3. Restart Oracle manually
4. Issue SQL restart commands using scripts from team laptops
5. Business team members test Dev & QA systems for proper operation using departmental restart checklist
6. Restart Dev and QA VM hosts
7. Restart Dev and QA VM guest OS

If you have any questions related to either of these procedures, please call the IT department.

After normal working hours or during weekends, contact John Q Public at 855.555.2121 or by email at JohnQ@WeFixIt.com.

All IT manuals are kept in <location>.

Inventory of IT equipment

Please complete for all Staff Computer Equipment in use at this location

Examples

Equipment	Model No.	Location	Under Contract		Contract #
Lenovo Laptop	i7-4510U	Bill's Office	☑ Yes	☐ No	DRB4- 0098
Brother Printer	DCP 7404	Main Desk	☐ Yes	☑ No	<_____>

Staff IT Equipment

<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

Public Use IT Equipment

Equipment	Model No.	Location	Under Contract		Contract #
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

Inventory of Office Equipment

Examples

Equipment	Model No.	Location	Under Contract		Contract #
Kodak Copier	ESP-5	Main Desk	☑ Yes	☐ No	RROB4- 0098
HP Scanner	Deskscan 12	Main Desk	☑ Yes	☐ No	PO100098

Second Floor Offices

<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

Inventory of Public Use Office Equipment

Example

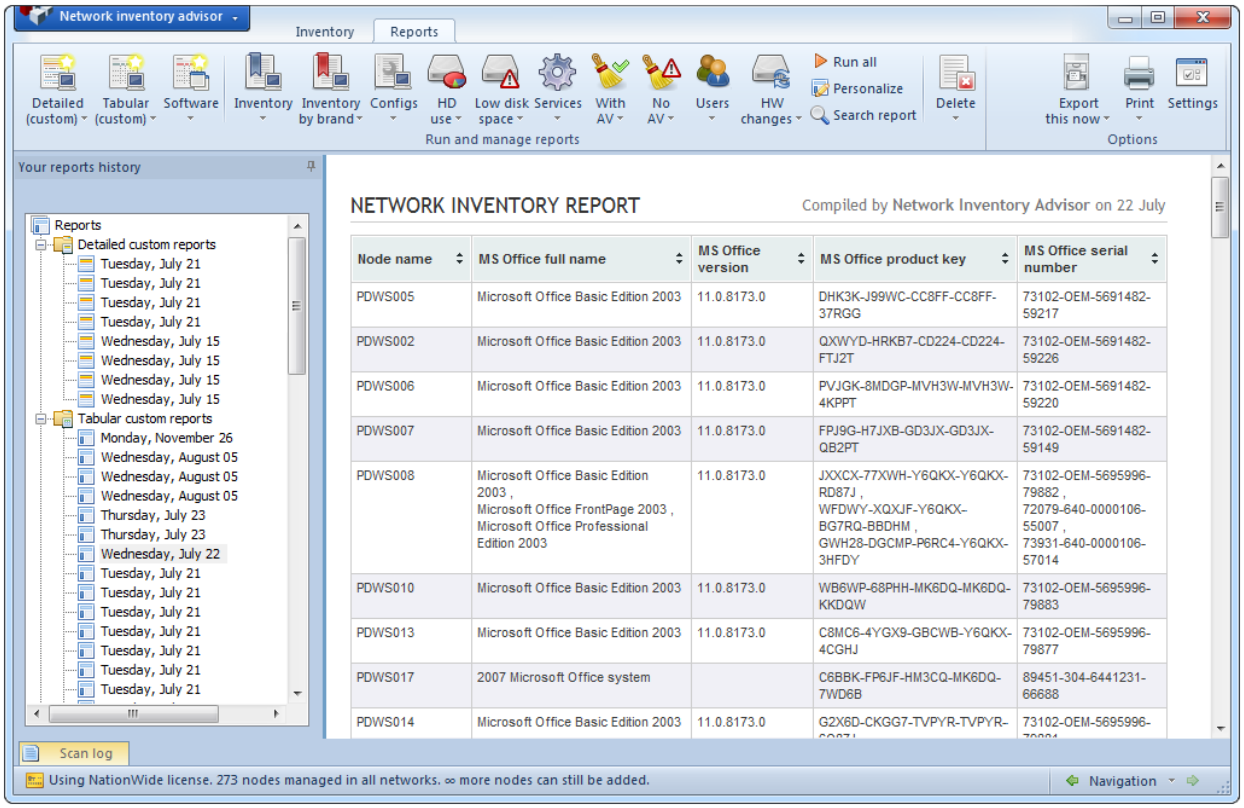
Equipment	Model No.	Location	Under Contract		Contract #
Apex LCD Projector	21-LCD 90	Conf. Room 3	☐ Yes	☑ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

Inventory of Security Equipment

<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>
<_____>	<_____>	<_____>	☐ Yes	☐ No	<_____>

Manuals for the above equipment are in storage cabinet 3 on the second floor.
The following is a list of our current software licenses. This list was compiled automatically using our new network discovery tool.

A print out of this list is maintained in storage cabinet 3 on the second floor, with the equipment manuals.



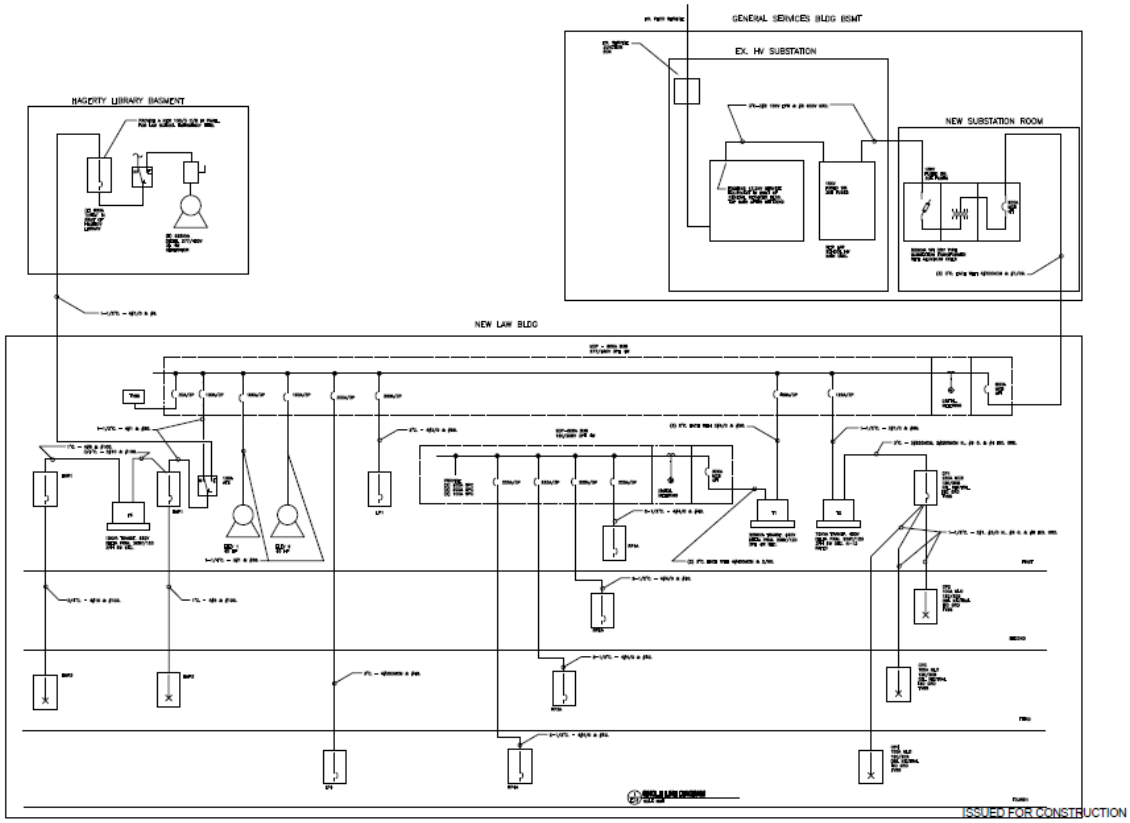
Standby Power Generator

The library has a Generac Guardian 11kw Standby Generator located several feet from the rear wall. Cabling for the generator is connected to the main power distribution system located in the basement. Instructions on starting the generator are located on the inside door. The key to the generator is located in the Head Librarian's office in the Key Control cabinet.

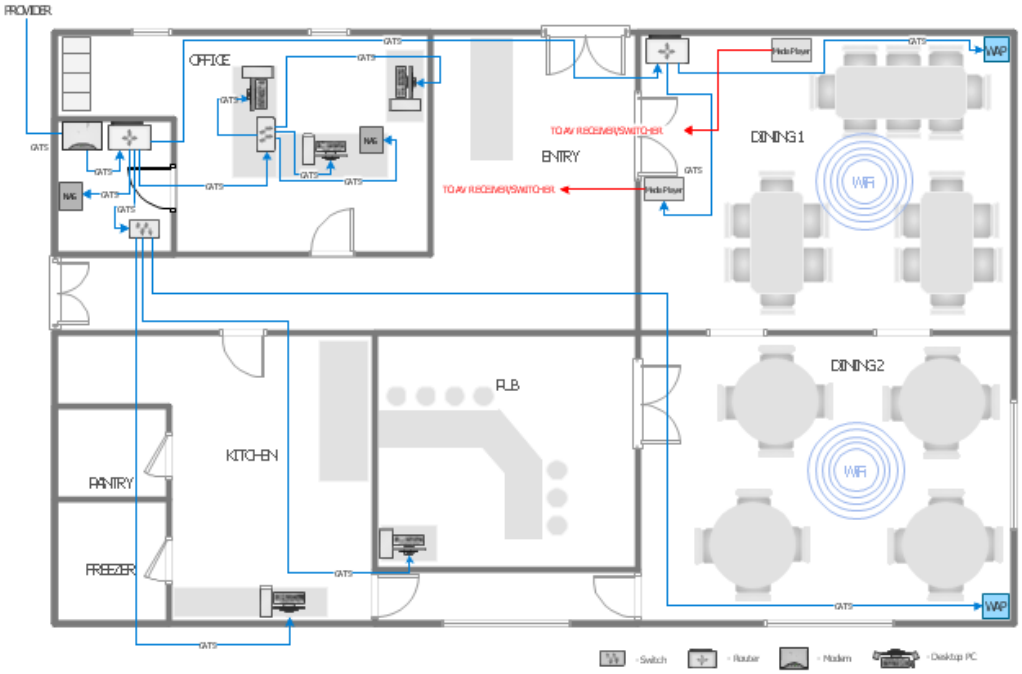
Directions for engaging the generator are located on the power panel in the basement.

The Generac Guardian has the ability to run a 3-ton air conditioner, well pump or water heater, and the main circulation rooms of the library. Additionally, power cords can be set out as charging stations for library patrons.

Appendix A - Library Power Diagram



Appendix B – Plumbing Diagram



Section A-3: COOP

Continuity of Operations Plan (Template)

Last Updated: (DD/MM/YYYY)

(Insert library Logo)

(Street Address)
(City, State, Zip Code)
(GPS Coordinates)
(Telephone)

COOP Background and Authority

FEMA offers a PDF template of a Continuity of Operations Plan (http://www.fema.gov//media-library/assets/documents/90025) which can be downloaded and used by non-federal agencies.

It provides a framework for non-federal agencies to develop a COOP that meets the standards outline in *Continuity Guidance Circulars 1 and 2* (July 2013).

This guide has not made any modifications to this plan since review and approval of continuity of operations plans by FEMA is a pre-requisite for obtaining certain types of aid during a crisis. Rather than make changes, each library is advised to visit the FEMA site and use the tools provided.

Household and Family Preparedness Planning

FEMA offers an easy to use family and household preparedness planning tool on their website (http://www.ready.gov/make-a-plan). Library staff should be encouraged to review this free tool and develop individual plans.

Section A-4:
Community Reengagement Plan

Community Reengagement Plan (Template)

Last Updated: (DD/MM/YYYY)

(Insert library Logo)

(Street Address)

(City, State, Zip Code)

(GPS Coordinates)

(Telephone)

Checklist of Community Resiliency Services

The following is a list of community stabilizing and outreach services that add significant value to communities impacted by a wide-scale event. These are services that would be of interest to commercial businesses, non-profit organizations, individuals and social groups.

Use this list as a starting point for the services that your library would prepare to offer in the aftermath of a disaster.

Onsite Services

- Once power is restored through the use of a standby generator or other means, libraries can act as warming or cooling stations for the public.
- Because of their design, libraries offer businesses, non-profits, and social groups flexible meeting spaces and a chance to pick up their lives and careers where they left off before the crisis occurred.
- One of the most needed services during a wide scale disaster is access to phone and computer charging stations. Once re-electrified, libraries can provide these services to large groups of people.
- Helping to restore a sense of security and normalcy is a critical role that libraries can fill. Story times for children, as well as restarting the lending program, conveys a sense that the community is recovering and things are on the mend.
- By acting as a central clearing house for information, libraries can help distribute various insurance forms and requests for aid. Librarians can even be trained to help people complete these documents and submit them in a timely fashion.
- As an information hub, it is very appropriate for libraries to collect and disseminate news. Some libraries do this in a very public way by projecting the latest information onto large walls inside the facility.

Outreach Services

- Through the use of mobile library trucks, community libraries can lend a helping hand by bringing outreach and on-the-go reference services to more heavily damaged communities areas.
- With some pre-planning, libraries can accommodate volunteer groups seeking to run food and clothing drives.
- Social media plays a key role in emergency response. Libraries can help connect local emergency staff and municipal officials with the public by pre-designating hashtags and other social media tags that the community can be told to consult when a disaster happens.
- Medical alerts or requests for specific donations can, in part, be managed by part of the library staff who can help organize pick-up and drop-off points.

What are the other needs of your community? Consider surveying local businesses and library patrons to solicit their feedback on needed services.

Section B: Additional Worksheets

General Security Checklist

		Yes	No
1.	Does your staff wear ID badges?	☐	☐
2.	Is a current photo part of the ID badge?	☐	☐
3.	Do you have a process for effectively cutting off access to facilities and information systems when an employee/contractor terminates employment?	☐	☐
4.	Are all parts of the building exteriors illuminated?	☐	☐
5.	Are the sides of the building easily visible from populated public areas?	☐	☐
6.	Are doorways well lit?	☐	☐
7.	Are all door and window locks well maintained and working?	☐	☐
8.	Is the landscaping around the building designed to eliminate blind spots?	☐	☐
9.	Are ladders and tools secured from unauthorized use?	☐	☐
10.	Is there a key management system in place?	☐	☐
11.	Are exterior doors fitted with tamper proof hinges?	☐	☐
12.	Where possible, are windows equipped with wire mesh guards?	☐	☐
13.	Is trash moved away so as not to be a fuel source for arsonists?	☐	☐
14.	Are security cameras visible and mounted high to prevent tampering?	☐	☐
15.	Have the local police been asked to drive by the facility regularly?	☐	☐
16.	Has outside equipment, such as A/C units, been secured?	☐	☐
17.	Are interior and exterior lights on a timer?	☐	☐
18.	Do all employees and volunteers receive safety and first aid training?	☐	☐
19.	Are background checks conducted on all employees?	☐	☐
20.	For child or youth programs is someone assigned to oversee safety?	☐	☐
21.	Is there a cyber-security protection plan in place?	☐	☐
22.	Are there policies that prevent unauthorized use of information systems?	☐	☐
23.	Are there policies that control physical access to secure areas, such as door locks, access control systems, security officers or video monitoring?	☐	☐
24.	Are your facilities and IT systems maintained by qualified experts?	☐	☐
25.	Have you had your facility inspected by law enforcement in the last year?	☐	☐

Dealing with Disruptive People Checklist

Signs and signals to be aware of when dealing with a potentially disruptive person.

Warning Signals: Trust Your Instincts

- □ Does the person enter the library in a loud disruptive manner?
- □ Is the individual trying to draw attention to their presence by speaking out in a loud voice, repeatedly asking questions or finding other ways to engage staff members?
- □ Do you feel uncomfortable with the content of the discussion?
- □ Do you feel uncomfortable with the language of the discussion? For example, are profanities being used?
- □ Do they seem angry?
- □ If angry, are their comments directed at a specific person who is present or at others?
- □ Is their conversation coherent or more like a rambling soliloquy?
- □ Is the person standing or sitting?
- □ Are they pacing or stumbling around as if on drugs or inebriated?

Be *Aware of Your Surroundings*

- □ Are you alone with the person or are other adults present?
- □ If alone, can you easily move to a more crowded area?
- □ Are young children in the immediate area?
- □ If children are present, can someone discreetly lead them to another area?
- □ Would you rather continue where you are or move the discussion to another area of the library?
- □ Can you motion to other staff members to join you in the immediate area?
- □ Can you discreetly signal for someone to call for assistance (e.g., security or 911)?

Try to Defuse the Situation

- □ Engaging the person in a conversation helps reduce tension.
- □ Understand that what begins as a conversation can escalate into a physical conflict at any time. Be prepared to take action to defend yourself and others.
- □ Begin by setting a peaceful, non-aggressive tone. Greet the individual with a smile and calm voice, but if you are uncomfortable do not approach them close enough to come into physical contact.
- □ If possible, once they have stopped, move to the side and speak to them from an angle. Avoid being directly face to face. Positioning yourself at their two o'clock or ten o'clock position is ideal. Stay far enough away so that you could not shake hands even if you wanted to. This will keep you safely out of range of sudden physical outbursts.
- □ Identify yourself and ask the person to do the same. For example: "I'm John Q. Public, one of the librarians. I don't think I know your name. How can I help you?" If the person refuses to answer,

continues to move forward, or becomes verbally agitated, these are serious warning signs that a physical confrontation is imminent.

- □ If the person stops, give them a moment to respond and then continue to ask for an explanation of their actions. Example: "Can I help you find something, answer a question, or direct you to something?"
- □ Avoid touching the person but indicate with hand motions that he or she should move to the side or sit down. Ask specifically, "Can I help you find someplace to sit and relax for a while?"
- □ If you get no reply, insist in a calm but firm voice that you would like to help them but need to know what they are looking to do. In doing so, offer them an option. Example: "We will be giving a news update in about 10 minutes. If you go over to the large meeting area there are some of our staff members who can help you get updated on things." If the person acquiesces, then you can decide if you want to accompany them or call ahead to put others on notice.

What to do if They Will Not Leave?

- □ Begin by approaching and greeting the individual. For example. "Hello. I'm sorry but it's closing time and we all have to leave the building. Even the staff has to leave and we do it together for safety purposes."
- □ Mention that the library will be open tomorrow and that they can return then, but do not make any comments about looking forward to seeing them again. This might be misinterpreted as interest on your part in starting a relationship.
- □ If they continue to move forward, say in a clear and strong voice: "I'm sorry, you must leave now or I am required to call for assistance."
- □ If the person gives no indication of leaving, take a moment and repeat your instruction to leave again, but a bit more forcefully such as: "I'm sorry, it's closing time and everyone must leave now. I have to join the rest of the staff for our nightly security walkthrough of the library."
- □ If they still do not move, step away and find help. Either have other staff members join you or call for assistance.
- □ Stay far enough away to avoid physical contact and do not approach them even if they ask for assistance. Instead, indicate that you are calling for some others to join you so that you can help the person find their way to the exit.

What to Avoid

- □ Do not get into a shouting match.
- □ Never let them touch you or approach close enough to touch you.
- □ Stand your ground, but be prepared to leave if that is an option.
- □ If the person becomes belligerent, stay only if you have no choice or if your leaving might put others in jeopardy.
- □ Treat the person with respect by listening to them and paying attention to their words, even if they are incoherent. Being ignored in a conversation may cause the person to turn violent.
- □ Be clear in your communication and you may find that what started as a problem will resolve into a solution.

If in a Crowd

On very rare occasions, a group of people may share a frustration and direct it at the library. Once again, this happens more often than not at closing time. The idea of leaving a place of light and safety for an uncomfortable evening in an area devoid of services can trigger a hostile response.

- □ Be careful of engaging in a conversation which begins to escalate into a debate.
- □ Watch to see if one individual seems to standout or take the lead. This person may assume the role of spokesperson/rabble rouser.
- □ If an individual does emerge as a leader, act to speak to them at another time or, at least, in another area where you can be more conversational. Isolating the person from the crowd may help calm things down.
- □ Do not put yourself in a position where you are alone or out of sight of others when you move to a different area. If in an office, leave the door wide open.

Summary Comments

In an ideal situation, how would you want to deal with this interruption? If confident that the person poses no threat, then you may choose to defuse the situation and deal with the individual as you would anyone in need of counseling or support. However, law enforcement professionals advise you to trust your instincts. If you feel that things may escalate take four steps:

1. Prepare yourself by putting aside any distractions such as text books, reports or other items.
2. Set up a screen between you and the individual. This might mean moving to a side location or offering to speak to them privately in another part of the room. Screening is especially important if you are with a vulnerable population such as the disabled, the elderly or children.
3. Instruct your staff to be on the lookout for these situations and to contact the police at the first signs of a problem. Remember, during a wide-scale crisis, law enforcement will be overtaxed with other duties and response times may suffer.
4. When speaking to the individual be sure to acknowledge that you are paying attention and listening to their comments, but avoid agreeing with any of their assertions or grievances. You want to be seen as someone who is part of the conversation but not a supporter of their position. Neutrality is the best policy.

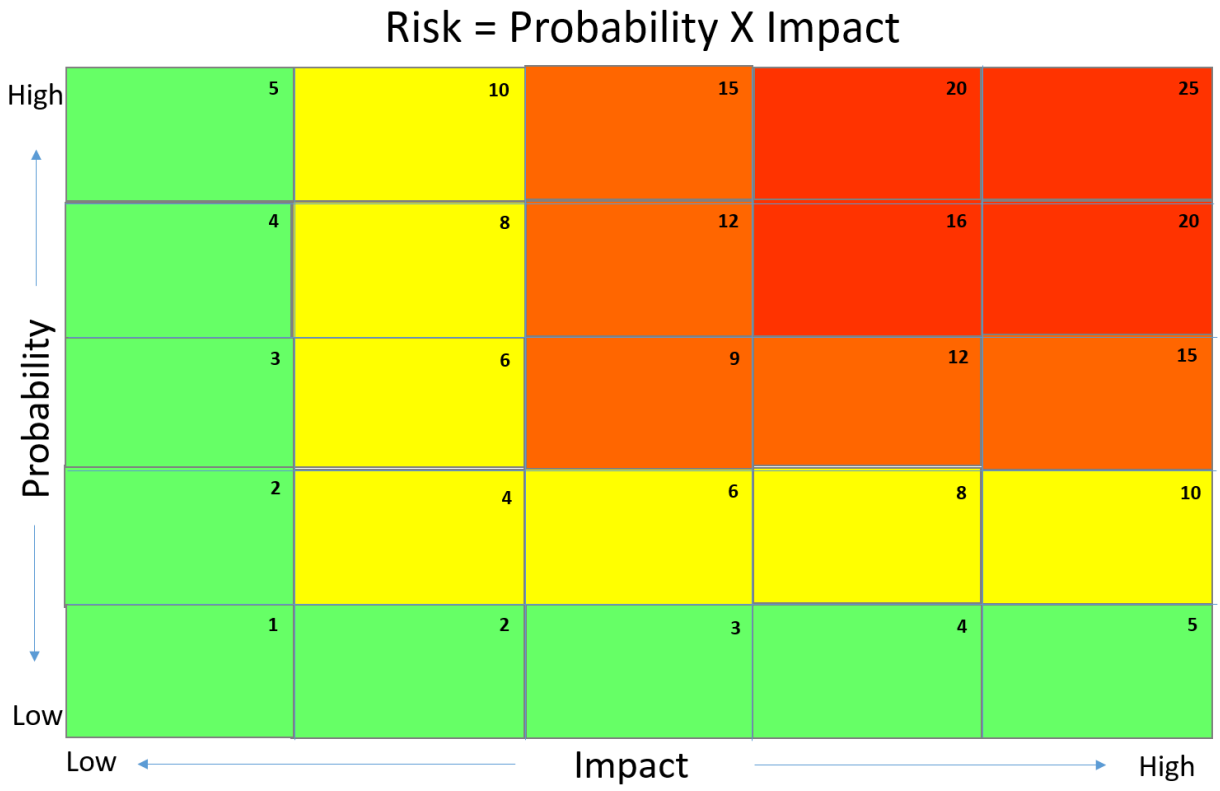
Risk Assessment Worksheet

Threat	Probability of Occurring in a Year (1 to 5)	X	Damage Impact ($)	=	Risk Score
State List					
1.< >	_		_		__
2.< >	_		_		__
3.< >	_		_		__
4.< >	_		_		__
Municipal List					
5. < >	_		_		__
6. < >	_		_		__
7. < >	_		_		__
Recent Threats					
8. < >	_		_		__
9. < >	_		_		__
10. < >	_		_		__

This done, map each of the high priority threats onto a Risk Matrix.

Risk Matrix

Mapping the identified risks onto the Risk Matrix highlights the areas that require attention and guidance on the correct Risk Control Strategy to apply.



Section C:
List of Identified Hazards by State

Introduction

Beginning in February of 2003 and continuing to the present, a series of Presidential Directives (HSPD-5 through HSPD-8 Annex 1) required all federal agencies to have a hazard mitigation plan. State and local government institutions also must comply with this requirement if they are to qualify for federal assistance during an emergency under the terms of the Stafford Act (Section 322 of 42 U.S.C. 5165).

The focus of these plans tends to be on natural hazards and not on failures of technology or human actions – although there are exceptions. For example, none of the fifty states cite the loss of network connectivity or the disruption of shipping services as hazards even though such events would shut down local commerce. However, New Jersey does recognize economic collapse as an issue and California cites train accidents and airline crashes as concerns.

The guidelines used to evaluate and select critical hazards are imprecise and subject to local interpretation. Even the terms used to identify hazards differ from state to state. For example, in some plans the word *conflagration* is used to describe a widespread fire while other states refer to this same threat as an *urban fire.*

The following is a complete listing of the hazards identified in the plans of all fifty states as of November 2014. While state plans are periodically updated these hazards will continue to represent key areas of concern for officials in these states for years to come.

Alabama

Flooding	Drought	Lightning
Landslides	Winter Storms	Dam Failure
Windstorms	Tornadoes	Tsunamis
Wildfire	Sinkholes	Sea Level Rise
High Winds	Earthquakes	Land Subsidence
Hurricanes	Hail	Extreme Temperatures

Alaska

Floods	Earthquakes	Dams
Community Conflagration	Tsunamis	Hazardous Materials
Wildland Fires	Severe Weather	Terrorism
Community Fire Conflagration	Ground Failure	Volcanoes

Snow Avalanches	Erosion	Economic Turmoil
Seiches (Standing Wave)	Hail	

Arizona

Dam Failure	Hail	Terrorism
Disease	Hazardous Material Event	Thunderstorm
Drought	Landslide	Tornado
Earthquake	Lightning	Tropical Cyclone
Extreme Heat	Severe Winds	Wildfire
Flood	Subsidence	Winter Storm

Arkansas

Dam Break	Landslide	Snow and Ice
Drought	Hail	Wildfire
Earthquake	Tornado	Wind
Flooding		

California

Earthquake Hazards	Water Shortages	Marine Invasive Species
Flood Hazards	Extreme Heat	Radiological Accidents
Wildfire Hazards	Freeze	Terrorism
Levee Failure	Severe Weather	Volcanoes
Landslides	Severe Storms	Air Pollution
Other Earth Movements	Dam Failure	Airline Crashes
Tsunami Hazards	Energy Shortage	Civil Disturbances
Climate related Hazards	Epidemic/Pandemic	Cyber Terrorism
Avalanches	Hazardous Materials Release	Hurricanes
Coastal Flooding	Oil Spills	Train Accidents
Erosion	Gas Pipeline Hazards	Explosions
Sea Level Rise	Insect Pests	Chemical Releases
Droughts		

Colorado

- Drought
- Extreme Heat
- Flood
- Hail
- Lightning
- Severe Wind
- Tornado
- Winter Storm
- Avalanche
- Earthquake
- Erosion and Deposition
- Expansive Soil
- Landslide
- Mud/Debris Flow
- Rockfall
- Subsidence
- Wildfire
- Pest Infestation

Connecticut

- Thunderstorm hazards
- Tropical Cyclone
- Tornado
- Winter Hazards
- Flood hazards
- Sea Level Rise
- Dam Failure
- Wildland Fire
- Drought hazards
- Earthquake

Delaware

- Flood
- Hurricane Wind
- Thunderstorm
- Tornado
- Hail
- Winter Storm
- Drought
- Earthquake
- Dam Failure
- Levee Failure

Florida

- Flood Profile
- Tropical Cyclones Profile
- Severe Storms
- Tornadoes Profile
- Wildfire Profile
- Drought Profile
- Extreme Heat Profile
- Winter Storms
- Freezes Profile
- Erosion Profile
- Sinkholes,
- Tsunami
- Solar Storm
- Technological Hazards
- Human-caused Hazards
- Terrorism Profile
- Severe Weather
- Tornadoes
- Flooding
- Tropical Storm
- Hurricane
- Wildfire
- Winter Storms
- Freezes
- Erosion
- Sinkholes
- Seismic Events
- Tsunami
- Solar Storm
- Technological Hazards
- Hazardous Materials
- Nuclear Power Plant
- Mass Migration

Earthquakes	Drought	Terrorism
Landslides	Extreme Heat	

Georgia

Tropical Cyclonic Systems	Tornadoes	Wildfire
Storm Surge	Inland Flooding	Seismic Hazards
Wind	Severe Winter Weather	Sinkholes
Severe Weather	Drought	Dam Failure

Hawaii

Hurricanes and Winds	Earthquakes	Landslides
Flood Hazards	Tsunami	Dam Failure
Drought	Volcanoes	Hazardous Materials
Wildfire	Airborne Hazards	Terrorism
Climate Change	Coastal Erosion	Health related Hazards

Idaho

Flood	Canal Failure	Severe Storms
Earthquake	Drought	Volcanic Eruptions
Avalanche	Hazardous Material	Wind Storms
Dam Failure	Landslides	Tornadoes
Levee Failure	Lightning	

Illinois

Severe Storms	Levee Failure	Extreme Heat
Tornadoes	Severe Winter Storms	Earthquakes
Floods	Drought	

Indiana

Tornado	Severe Thunderstorm	Winter Weather
Flood	Hail	Hazardous Materials Release
Dam Failure	Lightning	Structural Failure

Levee Failure	High Wind	Fires
Earthquake		

Iowa

Flooding	Contagious Diseases	Extreme Heat
Tornadoes	Dam Failure	Fire
Winter Storms	Radioactive Materials Release	Windstorms
Levee Failures	Terrorist Attacks	Sinkholes
Thunderstorms	Drought	Landslides
Lightning	Diseases and Epidemics	Other Ground Failure Hazards
Hailstorms	Transportation Incidents	Earthquakes
Animal Health	Infrastructure Failure	Expansive Soils

Kansas

Extreme Temperatures	Lightning	Tornado
Flood	Major Disease Outbreak	Utility Failure
Fog	Radiological	Infrastructure Failure
Hailstorm	Soil Erosion and Dust	Wildfire
Hazardous Materials	Terrorism	Windstorm
Land Subsidence	Agri-terrorism	Winter Storm
Landslide	Civil Disorder	

Kentucky

Drought	Hail	Severe Winter
Dam Failure	Landslide	Storm
Earthquake	Mine Subsidence	Tornado
Extreme Heat	Severe Storm	Wildfire
Flooding		

Louisiana

Flood	Ice Storm	Dam Failure
High Wind	Storm Surge	Levee Failure

Hurricane	Subsidence	Hazardous Materials Incident
Tornado	Wildfire	

Maine

Dam Failures	Hurricanes	Erosion
Earthquakes	Wildfire Fire	Coastal Erosion
Severe Winter Storms	Urban Fire	Landslide
Severe Summer Storms	Tornadoes	

Maryland

Coastal Flooding	Extreme Heat	Conflagration
Coastal Storms	Flood	High Wind Thunderstorm
Storm Surge	Landslide	Non thunderstorm Wind
Hurricane/Tropical Storm	Thunderstorm	Winter Storm
Nor'easter	Lightning	Extreme Cold
Sea Level Rise	Hail	Snowfall
Shoreline Erosion	Tornado	Karst
Tsunami	Wildfire	Sinkhole
Drought	Brush Fire	Earthquake

Massachusetts

Inland Flooding	Hurricanes	Snow and Blizzards
Riverine Flooding	Nor'easter	Ice Storm
Dam Failure	Tropical Storm	Tsunami
Ice Jams	Thunderstorm	Earthquake
Decreased Sediment	Drought	Landslide
Coastal Erosion	Extreme Temperatures	Urban Fires
Shoreline Change	Tornadoes	Wildfire
Sea Level Rise	High Winds	

Michigan

Thunderstorms	Snowstorm	Airline Crash

High Winds	Underground Freeze	Ice Storm
Tornadoes	Flash Flood	Blizzard
Flooding	Ship Explosion	Sewer Main Break
Rainstorms	Wildfire	Hail

Minnesota

Flooding	Landslide	Disease Outbreak
Wildfire	Sinkholes	Structures and Vehicles Fire
Tornado	Land Subsidence	Nuclear Plant Incidents
Windstorms	Earthquake	Hazardous Material Incidents
Severe Winter Storms	Extreme Temperatures	Transportation Incidents
Lightning	Dam Failure	Ground Water Contamination
Coastal Erosion	Terrorism	Surface Contamination

Mississippi

Hurricane	Extreme Winter Weather	Dam Failure
Tornado	Earthquake	Levee Failure
Flood Risk	Wildfire	

Missouri

Tornado	Flooding	Fires
Severe Thunder	Earthquake	Dam Failure
Winter Weather	Extreme Heat	Hazardous Material Release

Montana

Wildland and Rangeland Fires	Severe Winter Weather	Dam Failure
Flooding	Communicable Disease	Landslides
Earthquakes	Hazardous Material Incidents	Terrorism and Violence
Severe Summer Weather	Drought	Volcanic Eruptions

Nebraska

Severe Thunderstorm	Chemical Transportation	Earthquake

Severe Winter Storm	Transportation	Radiological Transportation
Power Failure	Chemical Fixed Facility	Dam Failure
Tornado	Agri-plant Disease	Levee Failure
Drought	Urban Fire	Civil Disorder
Flood	Wildfire	Radiological Release
Flash Flood	Terrorism	Public Health Emergency
Agri-animal Disease		

Nevada

Drought	Landslide	Canal Failure
Greater than 6.0 Earthquake	Lighting	Avalanches
Floods	Wind Storms	Seiches (Standing Wave)
Wildfires	Severe Winter	Tornadoes
Land and Ground Subsidence	Dam Failure	Volcanic Ash

New Hampshire

Flooding	Earthquake	Tornado
Coastal Flooding	Wildfire	Downburst
Drought	Landslide	Hurricane
Dam Failure	Radon	Tropical Cyclones

New Jersey

- Coastal Erosion
- Dam Failure
- Levee Failure
- Drought
- Earthquake
- Flood
- Hurricane
- Tropical Storm
- Nor'easter
- Severe Weather
- Wildfire
- Animal Disease
- Civil Unrest
- Crop Failure
- Cyber Attack
- Economic Collapse
- Fishing Failure
- Hazardous Substances
- Nuclear Hazards
- Pandemic
- Power Failure
- Terrorism

New Mexico

- Dam Failure
- Drought
- Earthquakes
- Extreme Heat
- Expansive Soils
- Flood
- Flash Floods
- High Wind
- Landslide
- Land Subsidence
- Severe Winter Storms
- Thunderstorms
- Lightning
- Hail
- Tornadoes
- Volcanoes
- Wildland Fire
- Urban Fire

New York

- Avalanche
- Climate Change
- Coastal Erosion
- Drought
- Earthquake
- Extreme Temperatures
- Flood
- Hailstorm
- High Winds
- Hurricane
- Land Subsidence
- Landslide
- Severe Winter Storm
- Tsunami
- Wildfire
- Expansive Soils

North Carolina

Flood	Wildfire	Dam Failure
Hurricanes	Drought	Levee Failure
Tropical Storms	Extreme Heat	Earthquakes
Nor'easters	Winter Storms	Sinkholes
Severe Thunderstorms	Freezes	Landslides
Tornadoes		

North Dakota

Dam Failure	Severe Summer Weather	Urban Fire
Drought	Severe Winter Weather	Structure Collapse
Flood	Shortage Critical Materials	Wildland Fire
Hazardous Material Release	Infrastructure Loss	Windstorm
Homeland Security Incident	Transportation Accident	

Ohio

Flood	Levee Failure	Coastal Erosion
Tornado	Wildfire	Drought
Winter Storm	Seiche (Standing Wave)	Severe Summer Storms
Landslide	Coastal Flooding	Invasive Species
Dam Failure	Earthquake	Land Subsidence

Oklahoma

Tornado	Wildfire	Extreme Heat
Winter Storm	High Wind	Earthquake
Ice	Drought	Dam Failure
Flooding	Thunderstorm	Landslides
Sinkhole	Hail	Expansive Soils
Subsidence	Lightning	Special Events

Oregon

Coastal Erosion	Fire	Tsunamis
Droughts	Flood	Volcanic Hazards
Dust Storms	Landslides	Windstorms
Earthquakes	Debris Flows	Winter Storms

Pennsylvania

Coastal Erosion	Hurricane	Subsidence
Drought	Invasive Species	Sinkhole
Earthquake	Landslide	Tornado
Extreme Temperature	Lightning Strike	Windstorm
Floods	Pandemic	Wildfire
Ice Jam	Radon Exposure	Winter Storm
Hailstorm		

Rhode Island

Thunderstorms	Dam Failure	Conflagration
Winter Weather	Fire	Earthquake
Hurricanes Medium	Wildfires	Drought
Flood Medium	Forest Fire	Extreme Heat
Tornadoes	Structural Fire	Coastal Erosion

South Carolina

Hurricanes and Tropical Storms	Wildfire	Landslides
Coastal Erosion	Drought	Infectious Disease
Severe Thunderstorm	Hail	Nuclear Plant Mishap
Lightning	Winter Storms	Sea level Rise
Tornadoes	Earthquake	Tsunami
Flooding	Sinkholes	Terrorism

South Dakota

Floods	Drought	Hazardous Materials
Winter Storms	Tornadoes	Agricultural Pest
Wildfire	Windstorms	Agricultural Diseases

Tennessee

Flood	Extreme Temperatures	Sinkholes
Earthquakes	Thunderstorms	Land Subsidence
Severe Weather	High Winds	Wildfires
Drought	Winter Storms	

Texas

Floods	Coastal Erosion	Extreme Heat
Hurricanes and Tropical Storms	Dam Failure	Hailstorm
Tornadoes	Levee Failure	Land Subsidence
Drought	Earthquakes	Severe Winter Storms
Wildfires	Expansive Soils	Windstorms

Utah

Flooding	Wildfire	Earthquake
Drought	Dam Failure	Landslides
Severe Weather		

Vermont

Flooding and Fluvial Erosion	Hail	Technological Hazards
Severe Thunderstorms	Drought	Dam Failure
Severe Winter Storms	Wildfires	Terrorism
Ice Jams	Landslides and Rockslides	Invasive Species
Tornadoes	Earthquakes	Rock Cuts
Hurricanes and Tropical Storms	Infectious Disease	Nuclear Plant Failure

Virginia

Flooding	High Wind	Tornado
Winter Weather	Drought	Wildfire
Landslides	Earthquake	Karst Topography
Floods		

Washington

Avalanche	Tsunami	Dam Safety
Drought	Volcano	Hazardous Materials
Earthquake	Wildfire Fire	Pipelines
Flood	Animal, Crop	Communicable Disease
Landslide	Plant Disease	Terrorism
Severe Storm	Infestation Outbreak	Urban Fire

West Virginia

Flood	Drought	Karst Topography
Wind	Extreme Heat	Natural Resource Extraction
Thunderstorms	Wildfire	Dam Failure
Tornadoes	Landslides	Levee Failure
Hurricanes	Earthquake	Hazardous Material
Winter Weather	Land Subsidence	Nuclear Accidents

Wisconsin

Hail	Wildfires	Earthquakes
Lightning	Drought	Landslides
Tornadoes	Extreme Heat	Land Subsidence
High Winds	Winter Storms	Dam Failure
Flooding	Coastal Erosion	Climate Change

Wyoming

Dam Failure	Lightning	Space Weather
Drought	Liquefaction	Tornado

Earthquake	Technological Hazard	Wildfire – Urban Fire
Expansive Soil	Human Caused Hazard	Wind
Flood	Mine Subsidence	Windblown Deposits
Hail	Avalanche	Winter Storm and Blizzard
Landslide		

For More Information

To learn more about how each state is addressing identified hazards, use a search engine to find each state's Multi-Hazard Mitigation Plan.

Other online resources that can provide additional information on this subject can be found at:

Federal Emergency Management Agency: http://www.fema.gov

National Priorities List: http://www.epa.gov/superfund/sites/npl

National Oceanographic and Atmospheric Administration: http://www.noaa.gov

Section E: Glossary of Cyber-Security Terms

Adware: Software designed to force pre-chosen ads to pop up with such speed and frequency that they seem to be taking over everything, slowing down your system and tying up all your system resources.

Advanced Persistent Threat (APT): An attack in which an unauthorized actor, often a nation-state, employs highly sophisticated technology to gain and maintain surreptitious access to a network.

Authentication: The intention of an APT may be to steal data, or to cause damage to the network or organization, or to plant attack capabilities for future activation. Stuxnet is an example of an ATP which damaged equipment in Iran.

Back Door: A means of accessing a computer system or network that bypasses security and may run undetected for a prolonged period.

Black Hat: Someone who attacks and attempts to invade a computer network. Black Hats often share information about their exploits with other Black Hat crackers.

Bot: A software "robot" that performs an extensive set of automated tasks on its own. Search engines like Google use bots, also known as spiders, to search (crawl) through websites and catalog all information there. Black Hats may use a bot as they perform an extensive set of destructive tasks, as well as introduce many forms of malware into a network.

Botnet: A network of zombie drones under the control of a Black Hat organization. When Black Hats launch a Distributed Denial of Service attack, they will use a botnet under their control to accomplish it.

Bypass: A flaw in a security device.

Ciphertext: Data that has been encrypted.

Continuous Monitoring: A process designed to regularly assess information systems to determine if their complete set of planned, required, and deployed security controls are effective over time.

Cookies: A small packet of information from a visited webserver stored on your system by a browser.

Countermeasure: Any action or device that reduces a computer system's vulnerability.

Covered Critical Infrastructure: Infrastructure equipment and components that would be subject to protections and conditions outlined under the Cybersecurity Act of 2012.

Cracker: Originally derived from the term "safe-cracker," a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage. These are the Black Hats.

Cracking: The process of trying to overcome a security measure.

Crypto Keys: The algorithms used to encrypt and decrypt messages.

Cryptography: The art of converting information or hiding its meaning by converting it into a secret code before sending it out over a public network.

Decrypt: The process of converting encrypted information back into normal, understandable text.

Denial of Service Attack (DOS): An attack designed to overwhelm a website through the sheer number and frequency of access attempts. A successful Denial of Service attack can cripple any entity that relies on its online presence by rendering their website virtually useless.

Digital Signature: An electronic equivalent of a signature.

Distributed Denial of Service Attack (DDOS): An attack performed using zombie drones (also known as a botnet) under the control of Black Hats.

Domain Name: The textual name assigned to a host on the Internet.

Dumpster Diving: The act of rummaging through the trash of an individual or business to gather information that could be useful for a cyber-criminal to gain access to a system or find personal information to aid in identity theft or system intrusion.

Easter Egg: A non-malicious surprise contained in a program or on a circuit board installed by the developer.

Firewall: A security barrier designed to keep unwanted intruders "outside" a computer system or network while allowing safe communication between systems and users "inside" the firewall.

Gray Hat: A White Hat/Black Hat hybrid. Their mission is to expose flaws in system security.

Hacker: A term coined in 1946 by the Tech Model Railroad Club of MIT meaning someone who applies ingenuity to achieve a clever result. When computers came along, "hacker" became someone who would "hack" away on a program through the night to make it better. With the coming of personal computers, a hacker became someone who invades privacy and puts the safety of information in jeopardy. The term "hacker" has come to mean a Black Hat actor. More precisely, the term should be "cracker."

High Risk Application: A computer application that, when opened, can cause the user's system to become vulnerable to a Black Hat attack.

Hijacking: The taking control of a computer system by an unauthorized individual.

Internet Relay Chat (IRC): A large, multiple-user, live chat session.

Internet Service Provider (ISP): Any company that provides users with technical connection to the Internet.

Intranet: A computer network that connects to the Internet and follows the accepted protocol.

Intrusion Detection: A type of monitoring program or other technique designed to detect attempts to penetrate a computer system or network.

IP Spoofing: An attack on a network where the attacker is disguised as another user by means of broadcasting a false IP network address.

Keylogger: A type of spyware that logs every keystroke made on a computer and transmits it to the Black Hat cracker who can then recreate user names and passwords.

Keystroke Monitoring: The process of recording every character typed by a computer user on a keyboard.

Leapfrog Attack: Using a password or user ID obtained in one attack to commit another attack.

Logic Bomb: A malicious program which will execute when a certain criteria is met. Until the triggering event, the logic bomb remains dormant.

Malware: Any malicious program that causes damage, including viruses, trojans, worms, time bombs, or logic bombs.

Master Program: The program a Black Hat uses to remotely transmit commands to infected zombie drones.

One-time Password: A randomly generated password that can be used only once.

Packet: A discrete block of data sent over a network.

Packet Sniffer: A device or program that monitors data traveling over a network.

Password: A data string used to verify the identity of a user.

Password Sniffing: The process of examining data traffic for the purpose of finding passwords to use later in attacks that use fake identities to gain access to a network (a.k.a masquerade attacks).

Payload: The part of a malware program that actually executes its designed task.

Pen Register: A device that records the telephone numbers of calls received by a particular telephone.

Phishing: A form of social engineering carried out by Black Hats in electronic form, usually by email, with the purpose of gathering sensitive information. Often these communications will look legitimate and, sometimes, even like they come from a legitimate source, such as a social networking site, a well-known entity, or a bank.

Phreaker: Precursors of the original computer hackers, phreakers, or phone phreakers, came into prominence in the '60s and made their mark by circumventing telecommunications security systems to place calls, including long distance, for free.

Piggyback: Gaining unauthorized access to a computer system via another user's legitimate connection.

Piracy: The act of illegally copying software, music, or movies that are copyright-protected.

Polymorphic Virus: A virus that will change its digital footprint every time it replicates. Antivirus software relies on an evolving database of signatures and profiles to detect any virus that may have infected a system. By changing its signature upon replication, a polymorphic virus may elude antivirus software, making it very hard to eradicate.

Pretty Good Privacy (PGP): A freeware program designed to encrypt email.

Probe: An effort to gather information about a computer or its users for the purpose of gaining unauthorized access at a later point.

Risk Assessment: The process of studying the vulnerabilities, threats to, and likelihood of attacks on a computer system or network.

Rootkit: A malware program that once introduced will create a back door for a Black Hat, allowing remote, unauthorized entry at will.

Script Kiddie: A pre-written program used by hackers to break the security of a network or computer.

Smart Card: An access card that contains encoded information used to identify the user.

Sniffer: A program designed to capture information from a computer network.

Social Engineering: An effort made to deceive someone for the purpose of acquiring sensitive and personal information.

Spam: Unsolicited email, also known as junk email.

Spoofing: The art of misdirection. Black Hat crackers will often cover their tracks by spoofing (faking) an IP address or masking/changing the sender information on an email to deceive the recipient about its origin.

Spyware: Software designed to gather information about a user's computer use without their knowledge.

Time Bomb: A malicious program designed to execute at a predetermined time and/or date.

Trap and Trace Device: A device used to surreptitiously record telephone numbers dialed by a specific telephone.

Trojan: A malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there. Once introduced, a Trojan can destroy files, alter information, steal passwords or other information, or fulfill any other sinister purpose it was designed to accomplish.

Trojan Horse: An apparently innocuous program that contains code designed to secretly access information or computer systems (a.k.a. a Trojan attack).

Virus: A malicious program or code that attaches itself to another program file and can replicate itself and thereby infect other systems.

War Dialer: Software designed to detect dial-in access to computer systems.

Wardriving: The act of driving around in a vehicle with the purpose of finding an open, unsecured Wi-Fi wireless network. There are Warbikers and Warwalkers, too.

Warez: Software that has been stripped of its copy-protection and made available on the Internet for downloading.

White Hat: Ethical hackers who use their knowledge and skill to thwart the Black Hats and secure the integrity of computer systems or networks.

Worm: Similar to a virus in that it is a destructive self-contained program that can replicate itself. Unlike a virus, a worm does not need to be a part of another program or document. A worm can copy and transfer itself to other systems on a network, even without user intervention.

Zero Day Threat/Exploit: Is a cyber-attack launched against a previously unknown weakness or exploit. It is called a "day zero" exploit because the vendor must immediately fix the weakness and has "zero days" in which to accomplish this task.

Zombie/Zombie Drone: A malware program that can be used by Black Hats to remotely take control of a system so it can be used as a zombie drone for further attacks.

For More Information:

Visit: the Department of Homeland Security websites: https://www.dhs.gov/topic/cybersecurity and https://www.us-cert.gov/ncas/tips.