TEAM NORFOLK

Emergency Operations & Resilience Framework

Hazard-Specific Annex

Cyber [Public]

October 11, 2022

Team Norfolk Emergency Operations & Resilience Framework
Hazard-Specific Annex: Cyber (Public)

October 11, 2022

STOP! Before you read this Hazard-Specific Annex, be sure you are aware of all that is written in the Framework's BASIC PLAN and your respective Emergency Support Function (ESF) Annex(es). The Basic Plan is the foundational document on which all annexes are built and explains strategies for Command and Control, Situational Awareness, Resource Requests, Communications and more. Your ESF Annex lists partner agencies, roles and responsibilities, available resources and other critical information.

Purpose and Scope

The purpose of this Hazard-Specific Annex is to provide an organizational framework and response capability with which the city can respond to a cyber incident. It is designed to not only meet the legal mandates outlined by State and local code in the areas of emergency services and emergency management, but to do so with unity of effort among all participating agencies.

Background

As a local government, the City of Norfolk has a very complex IT Infrastructure to maintain the operations ranging from Public Safety operations to Norfolk Public Libraries, City Hall operations, Critical Infrastructure (SCADA), among others, where they are all interconnected by components primarily deployed and maintained by its very own IT Department. Despite the ratio of IT staff-to-projects, the City of Norfolk has been recognized as one of the top Digital Cities in the US which has focused on Open Data/Transparency, Cybersecurity, Connectivity (broadband and Wi-Fi), Efficiency, Resilience, Innovation and Strategic Planning."

Norfolk Public Schools (NPS) is the largest urban school division in the Commonwealth of Virginia and the seventh largest division overall. The division enrolls a racially and economically diverse population of approximately 30,000 total students supported by a staff of more than 4,600 employees in 52 facilities. Connectivity is crucial in the learning as well as the business and administrative environments. As such, NPS provides a full range of computer information systems, including Internet resources, for students and staff. NPS strongly believes in the educational value of such computer information systems and recognizes their potential in support of our curriculum and student learning goals.

Recent events such as the cyber attack in Allenton, PA, Ransomware at Colorado DoT, Ransomware at Baltimore County Public Schools, and City of Atlanta's Ransomware incident proves localities and school districts are at risk and not adequately equipped to detect and contain these types of threats.

Situation

The City of Norfolk, as well as other local government organizations have faced growing cybercrime threats from Trojans, to spear phishing, whaling, and ransomware attacks, as well as constant hacking attempts and probes from state-sponsored organizations worldwide.

- Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway.
- Deliberate threats come from national governments, terrorists, industrial spies and organized crime groups, hacktivists and hackers.
- Ransomware costs exceeded $18 billion (globally) in 2020
- Nearly 7 billion people were targeted for cybercrime in 2021
- Cybersecurity spending will reach $459 billion by 2025
- The cost of cybercrime will reach $10.5 trillion by 2025
- Cyber attacks are increasingly complex and ever-changing
- A cyber incident may ultimately result in physical consequences impacting a single infrastructure or multiple and interdependent infrastructures.
- The City of Norfolk and Norfolk Public Schools Information Technology Departments utilize many technology safeguards.
- Norfolk IT sends periodic Secure Our System (SOS) periodic reminder emails.
- Along with the City's Computer Acceptable Use policy, Norfolk requires Cybersecurity training.
- Lack of access to computer systems is a scenario in the City's Continuity of Operations Plan (COOP), which also lists prioritization for program restoration.

Vulnerability Assessment

Computer technology is a necessity for conducting the clear majority of city business. As such, cities are responsible for storing and protecting confidential personnel, financial and HIPAA-related information. Moreover, information related to public safety and critical infrastructure must also be protected.

Vulnerability is determined by end user awareness and safe practices.

One end user can defy all technology in place used to prevent attacks.

Assumptions

- A large-scale cyber incident may overwhelm government resources.
- Team Norfolk, and the region for multi-jurisdictional response, will use the National Incident Management System (NIMS) and the Incident Command Structure (ICS) to manage the incident.
- Team Norfolk and the region will mobilize resources and personnel as required by the situation.
- Initial response may be focused on the physical impact of a cyber security incident while the actual cause and impacts of the incident may remain undetermined for a period of time.

Concept of Operations

General

The City of Norfolk and Norfolk Public Schools Information Technology departments are responsible for setting the policies and standards to protect their respective local government and K-12 schools information systems infrastructure, as well as for contingency and response plans needed to expedite recovery.

Direction and Control

Cybersecurity incidents affecting the city government network will be managed by the City of Norfolk Department of Information Technology; likewise, Norfolk Public Schools Information Technology will lead the response efforts for any incidents impacting their systems. Chief Information Security Officer (CISO) or designee will serve as the Incident Commander. Norfolk Emergency Preparedness and Response will provide logistical support and otherwise assist with making necessary notifications.

State, Local, Tribal, and Territorial (SLTT) governments and private sector entities can receive assistance from federal agencies to investigate incidents, mitigate consequences, and help prevent future incidents.

- CISA is the lead agency for asset response, which includes protecting assets and mitigating vulnerabilities.
- FBI is responsible for threat response, which includes attributing, pursuing, and disrupting cyber actors and activity.
- Office of the Director of National Intelligence (ODNI) is the lead agency for intelligence support, which is accomplished through the Cyber Threat Intelligence Center

Situational Awareness

The Homeland Security Information Network (HSIN) will be used to facilitate information sharing and otherwise document the incident.

DHS Cybersecurity and Infrastructure Security Agency (CISA)
https://www.dhs.gov/CISA
CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. The mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

DHS regularly publishes a number of cyber alerts and bulletins, which you can subscribe to here: https://www.cisa.gov/uscert/ncas/alerts

DHS CISA's National Cyber Security & Communications Integration Center
https://www.us-cert.gov/nccic
A 24X7 cyber situational awareness, incident response, and management center which shares information among public and private sectors to provide a common operating picture of vulnerabilities, intrusions, incidents, mitigation, and recovery actions. The NCCIC may be alerted of security incidents for situational awareness purposes to better understand the scope of the incident.

Industrial Controls Systems – Cyber Emergency Response Team (ICS-CERT)
https://ics-cert.us-cert.gov
Operates within the NCCIC and is a key component of the DHS mission to secure control systems within the nation's critical infrastructure. ICS-CERT may be notified by NCCIC to respond to cyber incidents involving control systems if additional resources are necessary and/or appropriate.

DHS Homeland Security Information Network (HSIN)

- **Critical Infrastructure (CI)** [Account / Membership Required]
- **Virginia Fusion Center – Cyber Security** [Account / Membership Required]

FBI Cyber Watch (CyWatch)
https://www.dsac.gov/topics/cyber-resources
Cyber Watch (CyWatch) is the FBI's 24-hour command center for cyber intrusion prevention and response operations. CyWatch receives threat and incident reporting, assesses it for action, and engages with the appropriate components within Cyber Division, the field, and other intelligence and law enforcement agencies for action.

Multi-State Information Sharing and Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/
Improved the overall cyber security posture of state, local, tribal and territorial

governments. MS-ISAC provides two-way sharing of information and early warnings on cyber security threats, a process for gathering and disseminating information on cyber security incidents, promotes awareness of the interdependencies between cyber and physical critical infrastructure as well as between and among different sectors, coordinates training and awareness, and ensures that all necessary parties are vested partners in this effort.

Virginia Fusion Center (VFC)

Virginia Fusion Center (VFC) Shield
https://fusion.vsp.virginia.gov/shield/
One of Virginia's tools for the widest possible distribution of information, typically at the open source or public level.

The VFC also distributes slightly more sensitive cyber information at the For Official Use Only level (FOUO). This is done through an internal distro list they manage. You can email and request to be added to the distro list for cyber intelligence products, but it will require signing a Non-Disclosure Agreement (NDA) with the center first. Request to receive cyber products can be sent to VFC@vfc.vsp.virginia.gov.

Alert and warning

Once aware of a suspected or confirmed attack or intrusion, the Network Security Engineer will notify the Chief Information Security Officer.

The Chief Information Security Officer will make the appropriate notifications. See attached Cybersecurity Alert Escalation Procedures.

If/when the incident appears more severe the Department of Information Technology has the resources to effectively respond, the CIO will alert the Director of Public Safety and Director of Emergency Preparedness and Response.

When appropriate, and based on consultation with Information Technology, the Director of Emergency Preparedness and Response will notify the Virginia Fusion Center.

Once notified by the City's or Schools' IT department, the EOC's first point of contact will be to the Virginia Fusion Center, especially should state assistance be requested. 877-4VA-TIPS / 877-482-8477.

Operational Periods and Situation Reports;

Operational periods will be determined at during the first EOC briefing.

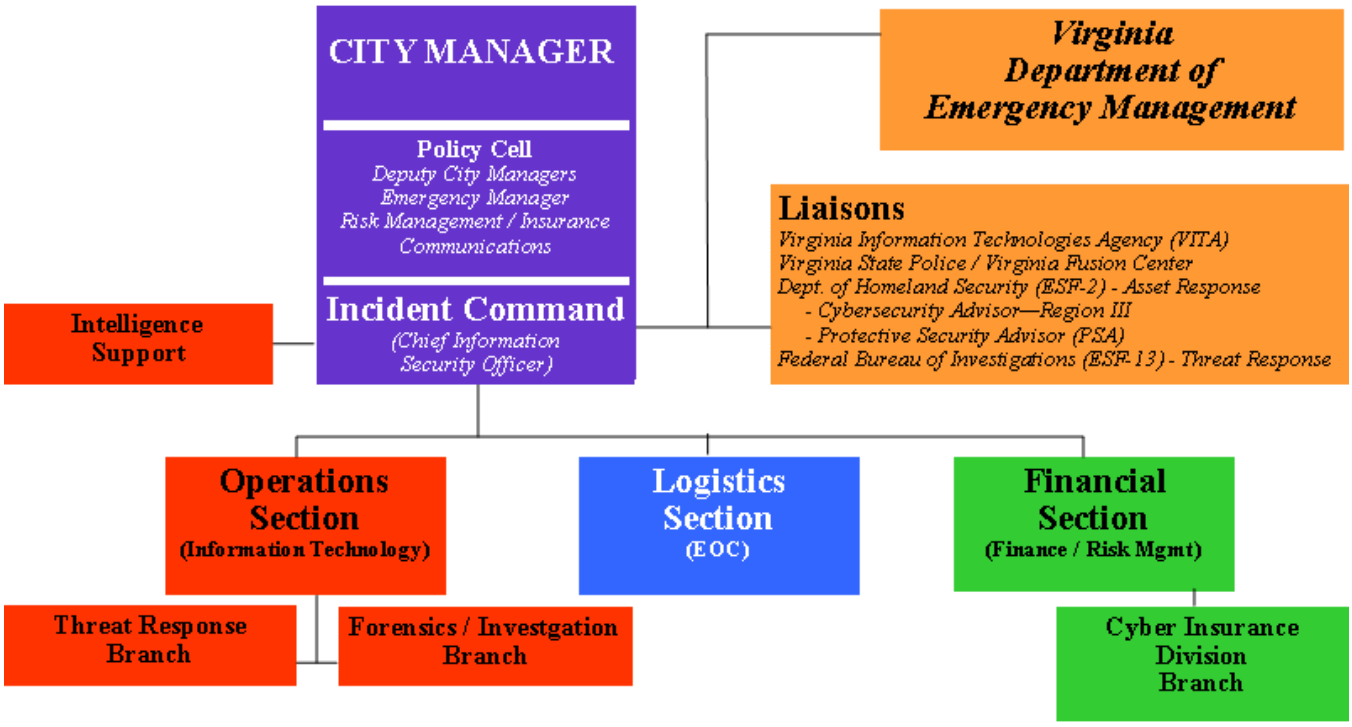
How the request for resources will be met;

Resource requests will be made by the Chief Information Security Officer and supported by the EOC Logistics Section.

Organization

For localized incidents, On-Scene Command will initially be established by the Chief Information Security Officer. If cascading effects or resource needs dictate, the Director of Emergency Preparedness and Response will assist the CIO in a Unified Command structure.

Cyber security incidents affecting local government infrastructure systems will be managed locally.



Roles and Responsibilities

CITY and SCHOOLS DEPARTMENTS

1. Department leadership and IT liaisons set the tone and expectation of adherence to cybersecurity policies and best practices.
2. Department IT Liaison personnel to ensure department systems are current and in line with IT Cybersecurity protection measures.
3. Ensure regular training occurs.

CITY and SCHOOLS STAFF

1. **Serve as the first line of defense against cyber intrusions.**
2. Maintain a culture of user awareness and technology vigilance.
3. Attend Cybersecurity training; maintain clean technology hygiene.
4. City staff who receive suspicious emails should forward them to reportspam@norfolk.gov or call the Help Desk immediately.
5. If you believe your computer / device / account has been compromised, contact the Helpdesk immediately.

Emergency Support Function 2.b Cyber

Norfolk Information Technology

1. Take preventive measures to protect the city's information network.
2. Develop and maintain a Cyber Strategic Plan.
3. Provide regular training to increase end user awareness.
4. Support Norfolk State University Cybersecurity Center of Excellence, Old Dominion University's Center for Cybersecurity Education & Research, Infragard Norfolk Chapter, and the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber).
5. **Lead and coordinate local cyber response efforts.**
6. **Notify the Emergency Operations Center of an ELEVATED INCIDENT.**

Remember the EOC has the ability through Norfolk Alert to send a blast message to Cyber partners and also schedule / facilitate a conference call briefings.

Norfolk Information Technology is developing a Computer Incident Response Team to provide rapid and effective response to cyber incidents.

Commonwealth of Virginia:

1. Cyber Security Advisor to serve as a resource to local governments.

U.S. Department of Homeland Security

1. National Cyber Security & Communications Integration Center (NCICC) to make notification to cyber response agencies.
2. FEMA Region III Cybersecurity Advisor to provide assistance upon request.
3. Protective Security Advisor to assist with coordination of resource support.

Emergency Support Function 5 Emergency Management

Emergency Preparedness and Response

1. Provides logistical support to the Incident Command.
2. Ensure the Policy Group, Virginia EOC, FBI and the DHS National Cyber Security & Communications Integration Center (NCCIC) are contacted.

Emergency Support Function 7 Logistics and Resource Support

Emergency Management

1. Provides logistical support to the incident command.

Emergency Support Function 13 Public Safety and Security

Norfolk Police Department

1. Assist with the investigation of criminal activity.

Virginia State Police – Fusion Center

1. Serve as the initial State-level point of contact for cyber incidents.
2. Coordinate and disseminate non-sensitive / non-identifying information to government and/or critical infrastructure partners.
3. Advises Cyber-UCG on recommended actions in response to a cyber incident.
4. Collect and analyze law enforcement information following an incident's conclusion.
5. Coordinates notification process and information flow to response partners.

Virginia State Police – High Tech Crimes Division

1. Serve as the lead agency for cyber criminal investigations within the Virginia Cyber Unified Command.
2. Provide investigative response and triage resources, as well as assist the post-incident criminal investigation and associated forensics upon request.

DHS Office of Cybersecurity & Communications (CS&C)

1. Work to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services.

2. Collaborate with the private sector – the ".com" domain – to increase security of critical networks.

Federal Bureau of Investigations (FBI)

1. Assist with Threat Response
2. Support investigations, intelligence gathering.
3. FBI Cyber Task Force - provide aid upon request
4. ***If there is a link to terrorism or the threat originated outside the United States, all investigatory responsibility will be assumed by the FBI.***

Emergency Support Function 15 External Affairs

Joint Information Center (JIC)

1. Ensure coordinated messaging among the response agencies.

Emergency Support Function 16 Military Affairs

Virginia Army National Guard

1. Conduct Network Security Assessments
2. Provide subject matter exerts and liaison officers upon request to assist with local response.
3. Provide incident response and recovery resources such as information assurances, applications, and network operations personnel, for affected state, local and private sector partners.
4. Collect, analyze, and share cyber threat and vulnerability information with appropriate agencies/entities on affected state, local and private sector critical infrastructures if available and appropriate.

Emergency Support Function 18 Education (Higher Education) /

Joint Forces Staff College / National Defense University

1. Partner and collaborate with Norfolk Information Technology to assist with end user awareness, share information and respond to local incidents.

Norfolk State University Cybersecurity Center of Excellence

1. Partner and collaborate with Norfolk Information Technology to assist with end user awareness, share information and respond to local incidents.

Old Dominion University Center for Cybersecurity Education & Research

1. Partner and collaborate with Norfolk Information Technology to assist with end user awareness, share information and respond to local incidents.

Resources

Commonwealth of Virginia: CyberVirginia
http://cyberva.virginia.gov/

Federal Cyber Incident Support (PPD-41)
https://www.cisa.gov/sites/default/files/publications/DHS%20Cyber%20Incident%20Response%20Fact%20Sheet%20v15%20-%20508%20Compliant.pdf

FBI Infragard
https://www.fbi.gov/about/partnerships/infragard

FBI Safe Online Surfing for Children
https://sos.fbi.gov

Homeland Security Critical Infrastructure Cyber Community C3 Voluntary Program
https://www.dhs.gov/ccubedvp
https://www.us-cert.gov/ccubedvp

Homeland Security National Cyber Security Awareness Month
https://www.dhs.gov/national-cyber-security-awareness-month

Stop. Think. Connect. Toolkit
https://www.dhs.gov/stopthinkconnect-toolkit

NASCIO Cyber Disruption Response Planning Guide (2016)

Ready.Gov: Cybersecurity: https://www.ready.gov/cybersecurity

Training Resources

Information Assurance Support Environment (IASE) Cybersecurity Online Training
https://iase.disa.mil/eta/Pages/index.aspx

IASE Cyber Awareness Challenge:
https://iatraining.disa.mil/eta/disa_cac2018/launchPage.htm

Texas A&M Engineering Extension Service (TEEX)
https://teex.org/Pages/Program.aspx?catID=231&courseTitle=Cybersecurity

Green or Low

Green is the lowest level in the cybersecurity threat matrix. The following will explain what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

Indicates that insignificant or no maliscious activity has been identified. Examples include but are not limited to:

- Credible warnings of increased probes or scans.
- Infected by known low-risk malware
- Other like incidents
- Normal activity with low level impact.

Actions:

- Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
- Continue routine security monitoring.
- Ensure all personnel receive proper training on Cybersecurity policies and best practices.

Escalation Criterion – This level is considered to be the IT baseline level where the infrastructure is operating normally and there are no major known cyber threats on the horizon.

De-Escalation Criterion – In order to return to this level the conditions that caused the change must be remediated.

Potential Impact – The threat level is low which means that there should be no cyber related issues impacting state IT resources. Note: Any type of IT disruption or anomalies should be reported to the EISO so it can look into the matter to determine if the disturbance is cybersecurity related or if it is caused by planned IT related functions like PATCH management or firewall reconfiguration.

Communication Procedures – Besides the day-to-day operational communications, there are no special communication procedures required while the state is at this level.

Blue or Guarded

Blues the first step in cybersecurity threat level. The following will explain what this level means and the impact it has on state government.

At this level, maliscious activity has been identified with minor impact. Examples include but not limited to:

- Change in normal activity with minor level impact.
- A vulnerability is being exploited and there has been minor impact.
- Infected by malware with the potential to spread quickly.
- Compromise of non-critical system(s) that did not result in loss of sensitive data.
- A distributed denial of service attack with minor impact.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems and implement appropriate counter-measures.
- Identify malware on system and remediate accordingly.
- Data exposure with minor impact.
- When available, test and implement patches, install anti-virus updates, etc. in next regular cycle.
- Contact MS-ISAC for any additional guidance.

Escalation Criterion – In order to raise the threat level to blue, the following conditions must be in place:

- Risk Level – The threat is limited to one agency, application, or website; and/or the risk of the threat is so low and it can be easily remediated without having a long-term impact to state, business partners, local governments, and citizens.
- Impact to IT Services – At level blue, the following conditions are in place:
    - Impact – There is no threat to mission critical applications or resources; and the issue has been properly identified and it can easily be remediated without risk of a data breach or theft of services.
    - Time – The issue can be remediated within normal business hours.
    - Remediation Effort – The threat can be easily remediated by the state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.
- Special Events/Circumstances – There is a special event or circumstance that might make hackers/ crackers interested in trying to disrupt the agency's IT services it or cause political embarrassment (Website Defacements, Application Hacking, etc.)

City Impact – IT staff will have to take some proactive measures (patches, updating anti-virus files, etc.) to address the potential issue but impact to IT services should be minimal since the threat has been identified there are ways to quickly address it without impacting IT services.

- Consider / activate the Computer Incident Response Team (CERT)

Communication Procedures – E-mail will be used to communicate alerts, status reports, updates, and ancillary information.

De-Escalation Criterion – In order to return to green, the issue must be completely resolved and the agencies confirm that the IT resources are working normally; and/or the special event has passed and there is no longer a need to take additional security measures.

Yellow or Elevated

Yellow or elevated is the third threat level in cybersecurity threat matrix. The following will explain what this level means and the impact it has on the state.

At this level, malicious activity has been identified with a moderate level of damage or disruption. Examples include but not limited to:

- An exploit for a vulnerability that has a moderate level of damage.
- Compromise of secure or critical system(s)
- Compromise of systems containing sensitive information or non-sensitive information.
- More than one entity (agency) affected in your network with moderate level of impact.
- Infected by malware that is spreading quickly throughout the Internet with moderate impact.
- A distributed denial of service attack with moderate impact.

Actions:

- Continue recommended actions from previous levels.
- Identify vulnerable systems.
- Increase monitoring of critical systems.
- Data exposure with moderate impact
- Contact CIO for additional guidance.
- Immediately implement appropriate counter-measures to protect vulnerable critical systems.
- When available, test and implement patches, install anti-virus updates, etc. as soon as possible

Escalation Criterion – In order to raise the state or agency threat level to yellow, the following conditions must be in place:

- Risk Level – The threat involves two or more agencies, critical applications, or websites; and/or the risk of the threat is has been determined to have a significant impact to state IT operations.

City Impact – At level yellow, the following conditions are in place:

- Impact
  - An exploit for a critical vulnerability exists and it has the potential to cause significant damage if exploited.
  - There are multiple web defacements.
  - A critical vulnerability is being exploited and there has been moderate impact.
  - Attackers have gained administrative privileges on compromised systems.
  - Critical applications or resources have been impacted.
  - Compromise of secure or critical system(s) containing sensitive information.
  - Compromise of critical system(s) containing non-sensitive information if appropriate.
  - IT Services may be interrupted by denial of service attacks.

- Time – The issue can be remediated within one to three business days and may require that the critical application or services be taken offline until the issue can be remediated.
- The Team Norfolk Continuity of Operations Plan/ Continuance of Government (COOP/COG) may have to be initiated to address the damages from the cyber attack.
- Remediation Effort – The threat can be remediated by the locality by installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges

Communication Procedures – Yellow or elevated situation means that some of the City's IT critical resources have been impacted by a cybersecurity event or that multiple agencies have had significant security breaches. At this level, the following communication mediums will be utilized:

- Director of Public Safety and Director of Emergency Preparedness and Response will be notified via email, telephone, or cell phone; Emergency Operations Center will start making preparations to enact the Team Norfolk Cybersecurity emergency response plan.
- E-mail – E-mail will be used to communicate alerts, status reports, updates, and ancillary information to the Senior Executive Team.

De-Escalation Criterion – In order to return to blue or guarded, the incident must meet the escalation criterion identified within that section; and/or the special event has passed and there is no longer a need to take additional security measures.

Orange or High

At this level, there are confirmed cyber attacks that are disrupting federal, state, and local government communications; and/or there are unknown exploits that have compromised the state's IT resources and are using them to propagate the attack or to spread misinformation.

At this level, malicious activity has been identified with a major level of damage or disruption. Examples include but not limited to: An exploit for a vulnerability that has a moderate level of damage.

- Malicious activity impacting core infrastructure.
- A vulnerability is being exploited and there has been major impact.
- Data exposed with major impact.
- Multiple system compromises or compromises of critical infrastructure.
- Attackers have gained administrative privileges on compromised systems.
- Multiple damaging or disruptive malware infections.
- Mission critical application failures but no imminent impact on the health, safety or economic security of the State.
- A distributed denial of service attack with major impact.

Actions:

- Continue recommended actions from previous levels.
- Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, etc. for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternative methods of communication in lieu of e-mail and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc. immediately.

Escalation Criterion – In order to raise the state or agency threat level to orange, the following conditions must be in place:

- Risk Level – The threat has the potential to impact multiple agencies and/or could require the City to shut down the IT infrastructure for five to ten business days to restore normal business operations.

City Impact – At orange, the following conditions are in place:

- Impact
  - A critical vulnerability is being exploited and there has been significant impact.
  - Telecommunications may be interrupted causing agencies to use alternate forms of communication (cell phones, radios, messengers, etc.).
  - E-mail communications may be disrupted making it necessary for agencies impacted by the event to use alternate forms of communication.

        - State CIO Executive Staff may have to be relocated to the state EMA for command and control purposes.
        - Agency IT Operations may have to be relocated to the state EMA for command and control purposes.
        - COOP may have to be implemented to restore IT operations.
        - Power may become unreliable/unavailable for extended periods of time.
        - Multiple damaging or disruptive virus attacks; and/or, multiple denial of service attacks against critical infrastructure services.
    - Time – The issue can be remediated within five – ten business days and may require that the critical applications or services be taken offline until the issue can be remediated.
    - The Team Norfolk Continuity of Operations Plan/ Continuance of Government (COOP/COG) will need to be initiated to address the damages from the cyber attack.
    - Remediation Effort – The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems, or applications to a previous date before the attacks occurred.

Communication Procedures – At orange the City's IT critical resources have been severely impacted by a cybersecurity event that has caused IT service offline for an extended period of time. This event may be impacting telecommunications and may cause incident responders to use alternate forms of communications (radios, satellite phones, messengers, etc.).

- Director of Emergency Preparedness and Response will be notified via email, telephone, cell phone or messenger and will start making preparations to enact the Team Norfolk Cybersecurity emergency response plan. In addition to this, the EMA will:
    - Convene a meeting among the CIO and the EOC Policy Group to assist with the recovery process.
    - Submit a situation report; submit resource request(s) to the Virginia Emergency Operations Center (VEOC) as appropriate.
    - Establish temporary communications (radio, messengers, etc.) for recovery personnel.
        - Consider the Hampton Roads Radio Cache

De-Escalation Criterion – In order to return to yellow, the incident must meet the escalation criterion identified within that section; and/or the special event has passed and there is no longer a need to take additional security measures.

Red or Severe

At this level, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks are being felt at a national, state, and local level.

At this level, malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but not limited to:

- Malicious activity results in widespread outages and/or complete network failures.
- Data exposure with severe impact.
- Significantly destructive compromises to systems, or disruptive activity with no known remedy.
- Mission critical application failures with imminent impact on the health, safety or economic security of the State.
- Compromise or loss of administrative controls of critical system. o Loss of critical supervisory control and data acquisition (SCADA) systems.

Actions:

- Continue recommended actions from previous levels.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.

Escalation Criterion – In order to raise the state or agency threat level to Red, the following conditions must be in place:

- Risk Level – The threat has the potential to impact multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.

City Impact – At red, the following conditions are in place:

- Impact
  - Telecommunications are unavailable making it necessary to use alternate forms of communication (radios, messengers, etc.).
  - The power grid is unreliable causing agencies to rely on the backup generators or UPS.
  - Buildings have been damaged or destroyed rendering IT resources inoperable.
  - State CIO Executive Staff have to relocate to EMA for command and control purposes.
  - COOP has to be implemented to restore IT operations.
  - Datacenters have to be restored or moved to their alternate facilities
- Time – The issues will take over ten business days to remediate and critical applications and services will be offline until the issues can be remediated.
- Remediation Effort – The threat can only be remediated by restoring the applications, systems, and facilities to an operational state by either rebuilding

equipment or restoring critical systems or applications to a previous date before the attacks occurred.

- The EOC has fully activated the Team Norfolk Cybersecurity emergency response plan.
- The Joint Information Center is activated.
- State and Federal resources are fully engaged in support of the locality.

Communication Procedures – At red the City's IT critical resources rendered inoperable by a cybersecurity that will take weeks to recover from. This event is impacting IT communications and necessitated the need for alternate forms of communications (satellite, radios, messengers, etc.).

- The EOC Policy Group maintains regular communication / meeting schedule.

De-Escalation Criterion – In order to return to orange, the incident must meet the escalation criterion identified within that section.