



**Brevard County, Florida  
Internal Audit of**

**Network Security Threat and Vulnerability Assessment**

**Prepared By:  
RSM McGladrey  
January 23, 2008**

# Table of Contents

---

Transmittal Letter .....	1
Background .....	2 - 8
Objectives and Approach .....	9 - 10
Network Security Threat and Vulnerability Assessment Findings .....	11 - 12

January 23, 2008

The Audit Committee of Brevard County, Florida  
2700 Judge Fran Jamieson Way  
Viera, Florida 32940-6699

Pursuant to the approved internal audit plan, we hereby submit our internal audit report covering the Network Security Threat and Vulnerability Assessment for Brevard County ("County"). The subject matter covered under this audit is confidential in nature, and thus specific details of any deficiencies are not disclosed to avoid the possibility of compromising County information and security. This exemption from Florida Statutes 119.07(1) and 286.001 and other laws and rules requiring public access or disclosure is addressed under Florida Statute 281.301, Security systems; records and meetings exempt from public access or disclosure. We will be presenting this public report to the Audit Committee at the next scheduled meeting on January 30, 2008 and all confidential matters have been communicated with appropriate personnel at the County.

Our report is organized in the following sections:

<b>Background</b>	This provides an overview of both the County's network infrastructure and the key elements for a network threat and vulnerability assessment.
<b>Objectives and Approach</b>	The internal audit objectives and focus are expanded upon in this section as well as a review of the various phases of our approach.
<b>Network Security Threat and Vulnerability Assessment Findings</b>	This section gives a high level description of the overall County Network Security Threat and Vulnerability Assessment findings.

We would like to thank the various members of the Information Technology (IT), Fire Rescue, Utility Services, E-911, and Emergency Operations departments involved in assisting the Internal Auditors in connection with the Network Security – Threat and Vulnerability Assessment.

Respectfully Submitted

***INTERNAL AUDITORS***

## **Background**

# Background

---

## **What is network security?**

Defining "network security" is not simple. The difficulty lies in developing a definition that is broad enough to be valid regardless of the network environment being described, yet specific enough to describe what security really is. In a generic sense, security is "freedom from risk or danger." In the context of computer science, security is the prevention of, or protection against, access to information by unauthorized recipients, and intentional but unauthorized denial of access to, destruction or alteration of that information.

This can be re-stated as-network security is the ability of a network to protect information and system resources with respect to confidentiality, integrity, and availability.

## **What is a Network Security Threat and Vulnerability Assessment**

Risks and vulnerabilities are often introduced into information systems because of incomplete, inadequate, or nonexistent security documentation. Security documentation, along with management support, is the cornerstone of any security program. We evaluated both management and operational practices related to network security to determine the potential risk within the County's network environment.

The overall purpose of a threat and vulnerability assessment is to assist an organization in the evaluation of its susceptibility to potential threats and identify corrective actions that can reduce or mitigate the risk of serious consequences from adversarial actions (e.g., system compromise, vandalism, equipment failure, insider sabotage, etc.). From a network security standpoint, the assessment included the use of specialized tools to probe computer networks in order to identify potential vulnerabilities that an attacker could exploit. Such an assessment takes into account the vulnerability of processes that are key to an organization's daily operations, while also considering risks related to damage towards, or attack on the County.

Technology vulnerabilities may be present in and apply to network services, architecture, operating systems, and applications. The vulnerabilities are comprised of the three following categories:

- Design vulnerabilities – a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability
- Implementation vulnerabilities – a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design
- Configuration vulnerabilities – a vulnerability resulting from an error in the configuration and administration of a system or component

# Background - continued

---

## Departmental Responsibilities

### Information Technology Department (ITD)

Unlike many other county agencies, the customers of ITD are mostly other internal county agencies and departments. ITD's main roles are to offer technology related services to help other county government agencies to do their work better, with improved efficiency, more reliable service. This department is also charged with maintaining the security and reliability of the county's network, computer and data systems.

ITD has the following functions:

- Telephone System Support - Provides telephone, wireless and other forms of communication services for employees
- Emergency 911 System Support - Works with other departments and local phone companies to ensure reliable address information is used in emergency calls
- Network Support - Provides a secure infrastructure for data communication within and outside of departments
- Help Desk Support - Ensures county employees are able to have problems resolved with computer equipment. PC technicians install, update and maintain equipment
- Application Development - Provides automation that allows government employees to do their jobs more efficiently. Provides applications, such as building permit search, for citizens
- Web Development - Hosts, develops and maintains 45+ websites. Provides technical expertise to other departments. Provides flexible content management services to meet employee and citizen needs

### Fire Rescue

Brevard County Fire Rescue offers a full range of fire suppression, advanced life support emergency medical service, public education, inspection, and special response team services throughout the communities in Brevard County. The Information Systems office supports all of the computer hardware, software, and network systems for Fire Rescue.

Fire Rescue IS handles the following functions:

- Build and/or maintain desktop and laptop workstations
- Maintain network servers
- Install and configure software operating systems and other computer software
- Maintain network connectivity between the computer servers and workstations
- Test and evaluate new hardware and software for better service to Fire Rescue employees
- Maintain and update Fire Rescue's internet website

# Background - continued

---

## Departmental Responsibilities - continued

### Utility Services

Brevard County's Utility Services Department provides and maintains sewer service to customers residing in many of the unincorporated areas of the County. The Department also operates a drinking water services for the residents of Mims, Barefoot Bay and Snug Harbor.

In addition to water and sewer service, Brevard County Utility Services is continually expanding a separate reclaimed water system which provides water for irrigating lawns and landscaping. This water, reclaimed by wastewater treatment plants rather than drawn from the ground, is distributed to homes, parks, fields, farms and golf courses around the County. Major components of the sewer and drinking water service include pumping stations and treatment plants.

- Pumping Stations - In order for gravity sewers to flow, they must be sloped downhill; however, at some point, the depth of the sewer becomes too great for practical installation and maintenance. In regions without hills, such as coastal Florida, pump stations are required periodically to elevate the water into a new gravity sewer. Sewage pump stations, also called lift stations, pump the water up to a new gravity sewer, thereby allowing gravity to transport the sewage downhill again. In 2006, Brevard County Utility Services operates 251 pumping stations.
- Treatment Plants - Water is the carrier vehicle used to transport our wastes away from our homes. The purpose of sewage treatment is to remove the harmful substances from the water so that it may be re-introduced into the environment without causing public health or environmental problems.

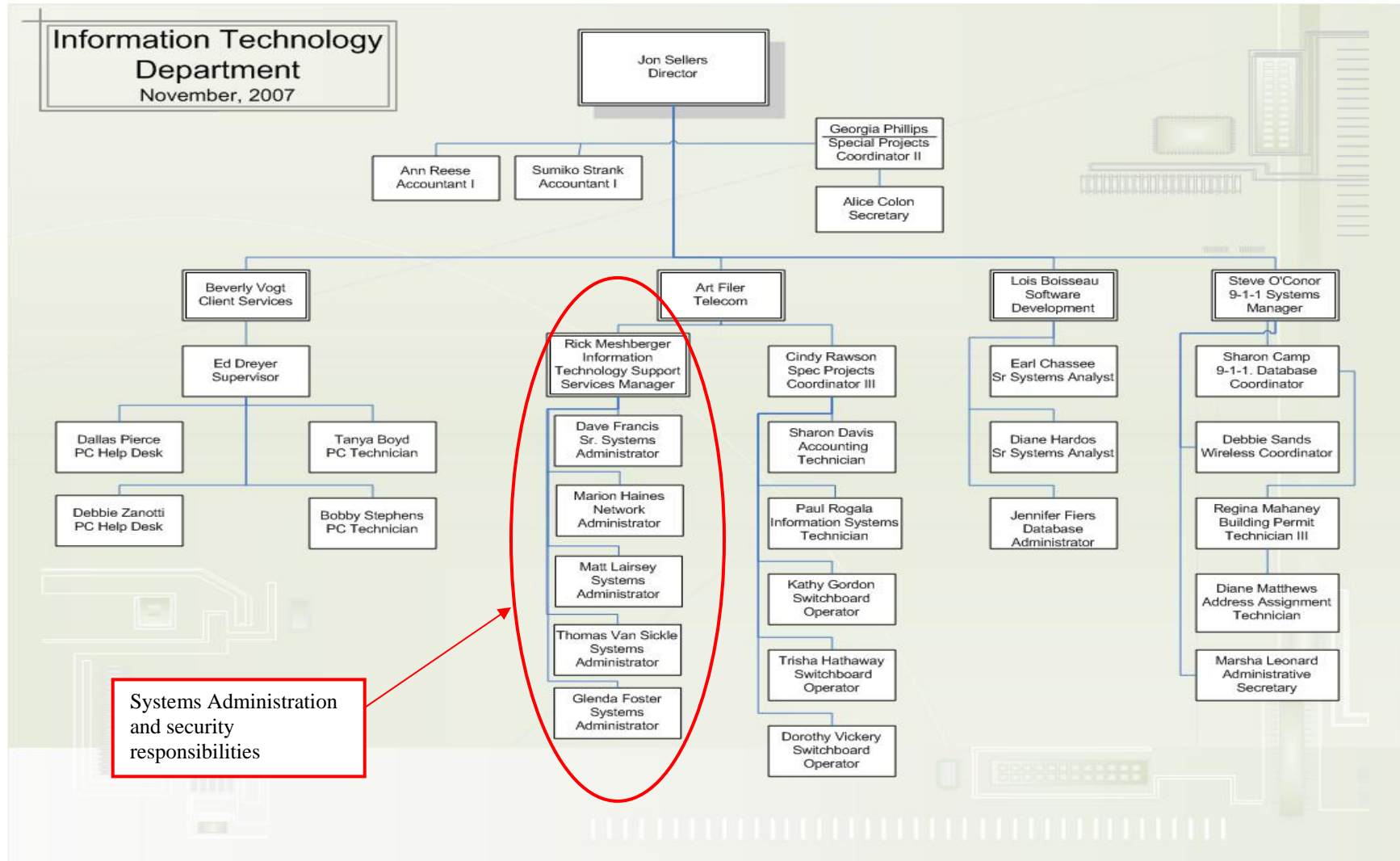
Electronic technology, computerization, instrumentation and communication play an important role in providing effective cost control and quality water and sewage services. Radio telemetry and control systems initially used in oil, gas and power industry were adapted to wastewater pumping and treatment systems. These systems are referred to as Supervisory Control and Data Acquisition systems or SCADA system. The Utilities Services Department operate these systems that monitor the six treatment plants, most of the 251 pumping stations, several booster stations for water and reclaimed water, as well as an elevated water tank and several wells.

During different stages of processing water, wastewater, and reclaimed water, instrumentation in the plants monitor and report key information regarding:

- Levels and flows
- Concentration of chlorine and acidity
- Clarity or turbidity

# Background - continued

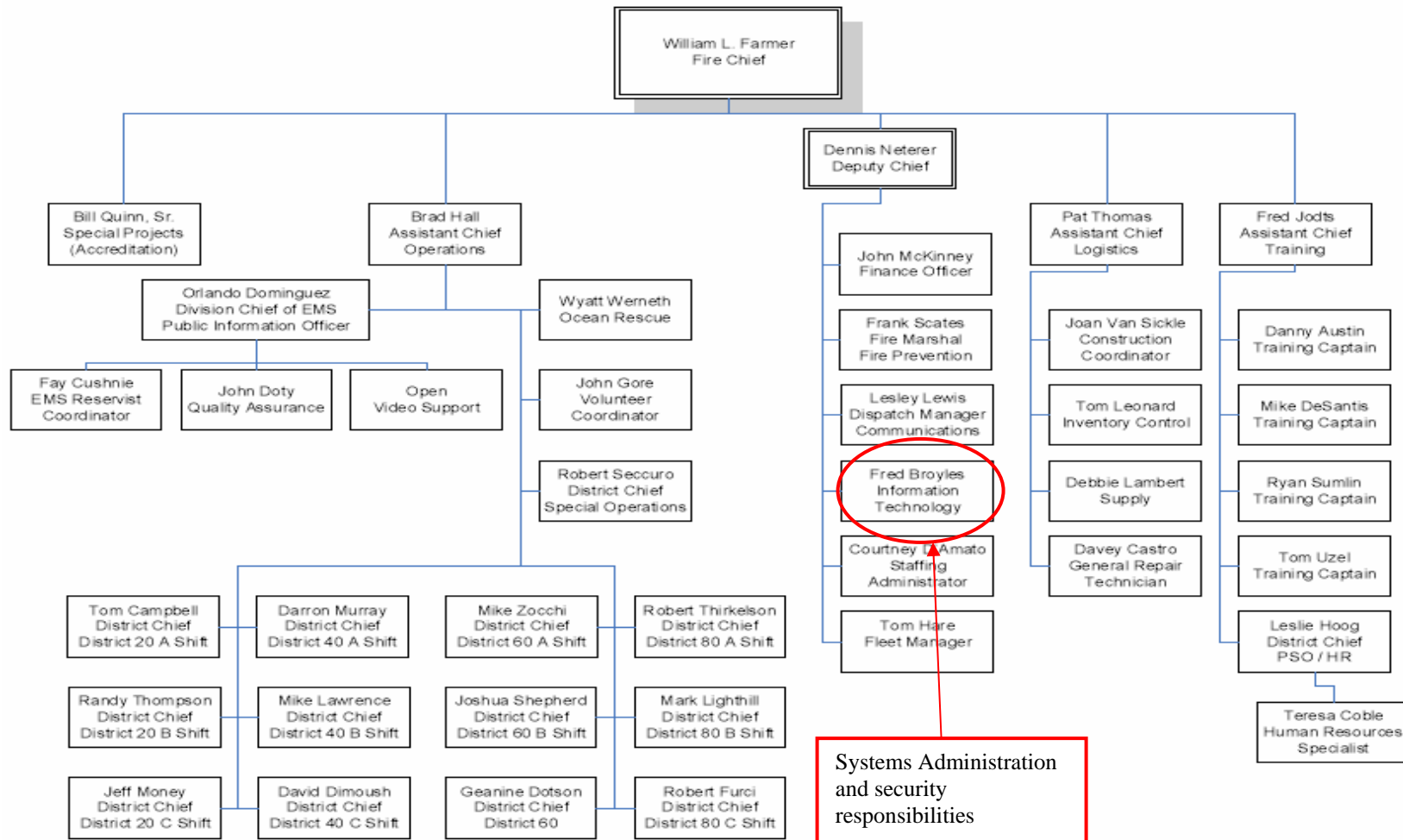
## Information Technology Department Organizational Chart



# Background - continued

## Fire Rescue Organizational chart

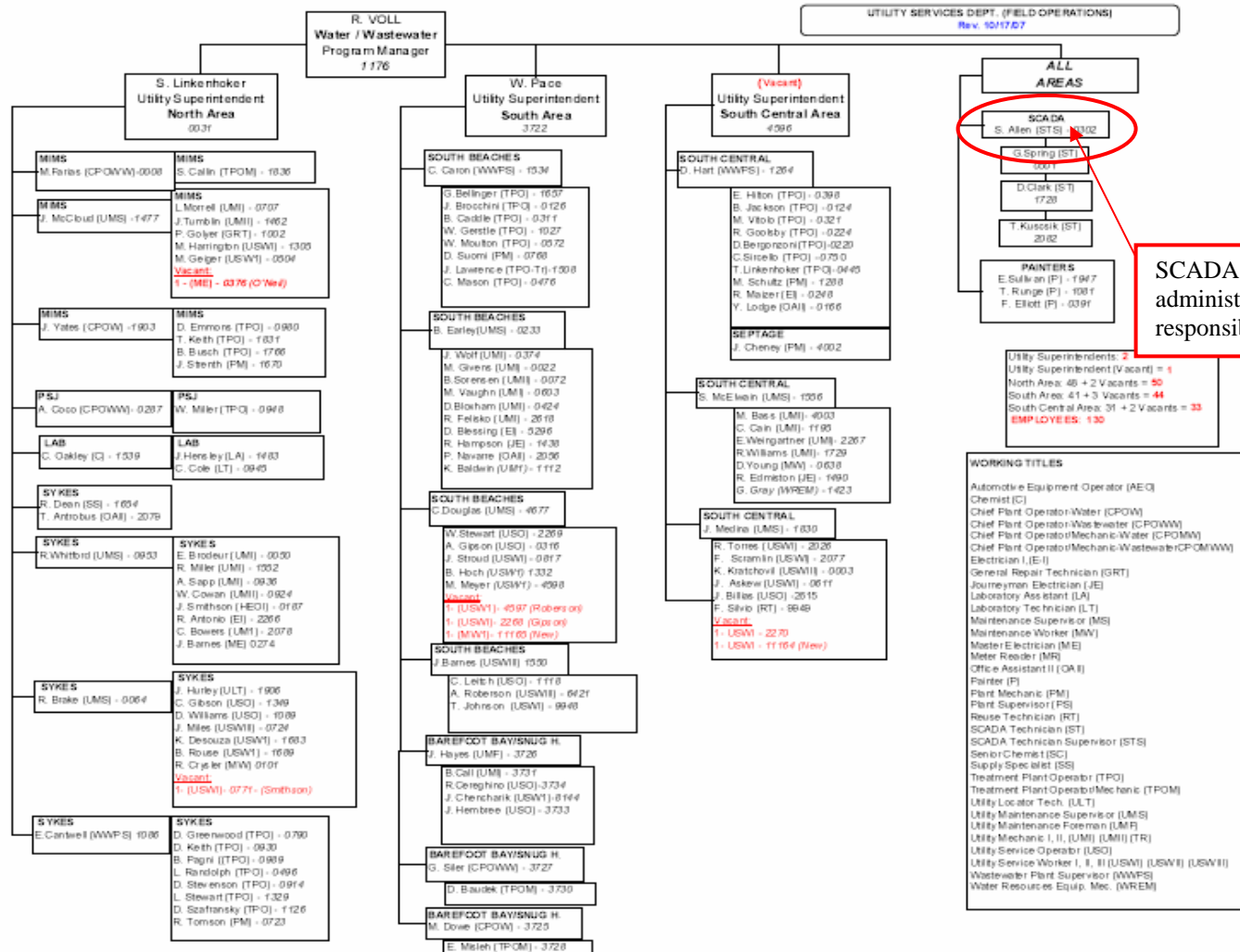
### Brevard County Fire Rescue





# Background - continued

## Utility Services Organizational Chart (Continued)



SCADA Operations and administration responsibilities

## **Objectives and Approach**

# Objectives and Approach

---

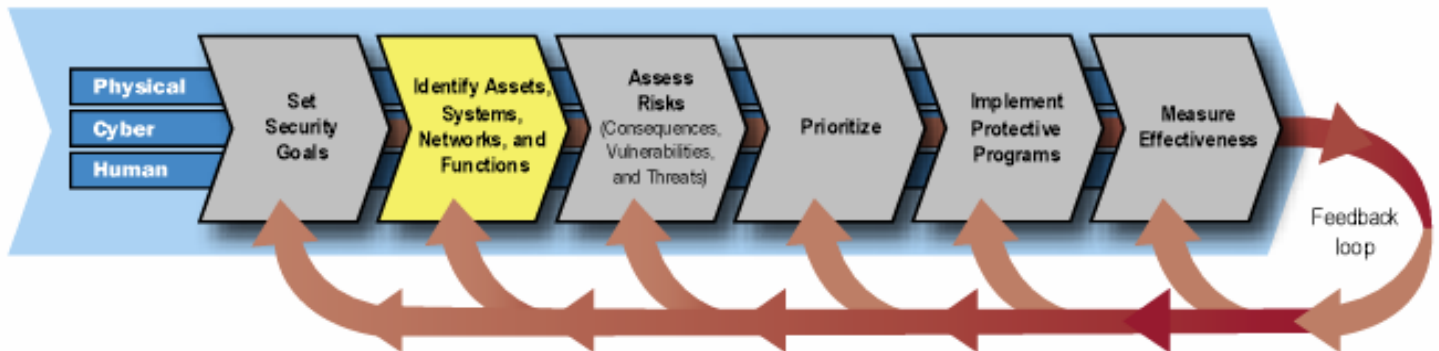
## Objectives

This assessment was focused on the County’s security risks regarding the networks supporting administrative, Fire Rescue, Emergency Operations, E-911 and Utility Services SCADA data processes. Objectives included the following:

1. Identify strategic and operational gaps in the following areas:
  - a. Vulnerability Management
  - b. Incident Management
  - c. Systems and Network Management
  - d. Contingency Planning / Disaster Recovery
  - e. Physical Security Plans and Procedures
  - f. Security Awareness and Training
2. Assess the threats and vulnerabilities present in the network environment. This included, but was not limited to, an analysis of:
  - a. Operating systems
  - b. Wireless networks
  - c. Applications
  - d. Databases

## Approach

Our audit approach consisted of following industry accepted practices derived from the Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) Method Implementation Guide and the OCTAVE Method. In addition, this approach is in line with the Department of Homeland Security National Infrastructure Protection Plan (NIPP) risk management processes.



## Understanding and Documentation of the Process

We conducted interviews with the key departmental staff responsible for application and network operations support services. We discussed the scope and objectives of the audit work, obtained preliminary data, and established working arrangements. We obtained copies of policies and procedures, organization charts, and network inventories, topology diagrams, budgets and other documents deemed necessary. We reviewed the applicable Florida Statutes and a preliminary review of the Management and Operational practices for the County’s application and network environment. A determination of the level of risk to the County for administrative, Fire Rescue, Emergency Operations, E-911 and Utility Services SCADA environments was developed based on the data and process sensitivity and criticality, as well as the exposure to external networks and other high risk environments.

# Objectives and Approach - continued

---

## Testing

In order to meet our outlined objectives we conducted extensive testing of the selected departments. Specifically, our testing included the following techniques:

- Extensive interviews with management and staff involved in both administrative and technology support activities.
- Review of applicable policies, procedures and records
- Network device analysis and testing
- Wireless scanning
- Host and network analysis and testing
- Data center and LAN closet walk downs
  - The following network segments and associated IP addresses were selected for testing:
    - External (publicly accessible) Network –
      - 2040 potential addresses
    - Administrative Network –
      - 9180 potential addresses
    - Emergency Operations Network –
      - 1275 potential addresses
    - Fire Rescue Network –
      - 549 potential addresses
- Wireless scanning to ensure no unknown or unauthorized wireless access points exist on the County's network
  - Using NetStumbler, a physical walkdown/evaluation of fourteen (locations) were selected for testing.
  - The testing methodology involved scanning the perimeter of each location and then moving inward to discount any wireless access points belonging to outside entities, such as surrounding homes and businesses.
  - The following is a list of locations that were evaluated;
    - Selected buildings of the Brevard County Government Complex
    - Emergency Operations Center
    - Selected Utility Services Facilities
    - Selected Fire Stations
- Data center and LAN closet walk downs
  - The following is a list of locations that were evaluated;
    - Fire Rescue Service Center
    - Emergency Operation Center
    - Utility Services SCADA

## Reporting

We prepared a matrix to report the high level findings in this public report. We conducted exit interviews with the County's management teams where we discussed the issues identified and action to date. As detailed in the transmittal, the subject matter covered under this audit is confidential in nature, under Florida Statute 281.301 and thus specific details of any deficiencies are not disclosed to avoid the possibility of compromising County information and security. All matters have been communicated in writing to the County Manager.

# **Network Security Threat and Vulnerability Assessment Findings**

## Network Security Threat and Vulnerability Assessment Findings

Following is a high level summary of the major issues identified during our internal audit. The subject matter covered under this audit is confidential in nature, and thus specific details of any deficiencies are not disclosed to avoid the possibility of compromising County information and security. This exemption from Florida Statutes 119.07(1) and 286.001 and other laws and rules requiring public access or disclosure is addressed under Florida Statute 281.301, Security systems; records and meetings exempt from public access or disclosure.

Rating		
<b>High</b>	<b>1</b>	<b><i>Security Program Management</i></b>
		<p>Security strategies, policies, and procedures are the roots of a sound security program. Currently, governance controls are not always in place to provide reasonable assurance that appropriate strategy, policies, and procedures are in place to maintain adequate levels of security management and oversight. This includes:</p> <ul style="list-style-type: none"> <li>• Defining security strategies</li> <li>• Allocated sufficient funds and resources to information security activities including:               <ol style="list-style-type: none"> <li>1. Defined security roles and responsibilities</li> <li>2. Defined risk management strategies</li> <li>3. Routine review security related reports</li> </ol> </li> <li>• Developing a comprehensive set of documented, security policies that are periodically reviewed and updated</li> <li>• Developing documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).</li> </ul>
<b>High</b>	<b>2</b>	<b><i>Vulnerability Management</i></b>
		<p>Currently, vulnerability management processes are not always in place. Also, network, host, and applications are not always configured and monitored to prevent and detect known vulnerabilities and could expose critical systems to external and internal attacks. Examples of network and application vulnerability risks are listed below:</p> <ul style="list-style-type: none"> <li>• Malicious network aware software installed on host systems</li> <li>• Insecure web application components, versions, patch issues, and potential code execution (cross site scripting) issues</li> <li>• Insecure or mis-configured network components and applications including Operating systems, network hardware, network aware applications and databases that could lead to a compromise</li> <li>• Default and commonly known user id and password combinations for operating systems, network hardware, network aware applications and databases</li> <li>• Peer-To-Peer File Sharing</li> </ul>
<b>High</b>	<b>3</b>	<b><i>Incident Management</i></b>
		<p>Currently, the County's IT incident management system is not integrated to ensure operational events that are not part of standard operations that could expose the organization to potential operational disruption are identified, assessed and responded to in a timely manner. Specifically, the absence of the integrated incident management processes could result in a lack of response to network and/or application incidents.</p>

## Network Security Threat and Vulnerability Assessment Findings - continued

Rating		
<b>Medium</b>	<b>4</b>	<b><i>Systems and Network Management</i></b>
	<p>Network segments are not always configured to reduce the likelihood of unauthorized use, disclosure of proprietary information, modification, damage or loss of data. Typical vulnerabilities in this area include the following activities:</p> <ul style="list-style-type: none"> <li>• Network devices placed behind firewalls</li> <li>• Authentication and authorization</li> <li>• Regular network monitoring and auditing</li> <li>• Use of system administration tools to facilitate securing, monitoring, and auditing activities.</li> </ul>	
<b>Medium</b>	<b>5</b>	<b><i>Change and Patch Management</i></b>
	<p>Change control and patch management processes are not always established. Uncontrolled system changes increases the risks of unauthorized use, disclosure of proprietary information, modification, damage, or loss of data.</p> <ul style="list-style-type: none"> <li>• Changes to IT hardware and software are planned, controlled, and documented.</li> <li>• All systems are up to date with respect to revisions, patches, and recommendations in security advisories</li> </ul>	
<b>Medium</b>	<b>6</b>	<b><i>Contingency Planning / Disaster Recovery</i></b>
	<p>A continuity of operations or disaster recovery plan has not been established for all departments reviewed to adequately address events that could result in disruption of critical operations. Normally business/operational continuity and disaster recovery vulnerabilities occur due to a failure in one or a combination of following processes:</p> <ul style="list-style-type: none"> <li>• Business/operational impact analysis</li> <li>• Periodic testing, verification and updating</li> <li>• Identify backup and restoration requirements</li> </ul>	
<b>Medium</b>	<b>7</b>	<b><i>Physical Security Plans and Procedures</i></b>
	<p>Physical security is not always in place to prevent unauthorized/uncontrolled access, physical modification and damage to critical assets. Physical security vulnerabilities, typically occur when the following activities are either not in place or not operating effectively:</p> <ul style="list-style-type: none"> <li>• Controls are in place to deter, detect and respond to inappropriate access and use of critical assets</li> <li>• Physical security procedures and mechanisms are routinely tested and revised</li> </ul>	
<b>Low</b>	<b>8</b>	<b><i>Security Awareness and Training</i></b>
	<p>Personnel in all departments reviewed are not always trained or provided direction needed to fulfill their responsibilities and that untrained staff may not use information assets and tools productively or efficiently. Specifically, that security awareness, training and periodic reminders are provided for all personnel.</p>	