



Department of Administration

Frank Pascarella, County Administrator

June 25, 2013

RE: County Adopts Government Campus Integrated Security Plan

On June 11, 2013 the Chippewa County Board of Supervisors adopted the Government Campus Integrated Security Plan.

In 2012, Chippewa County officials began an initiative to improve safety and security and to develop a comprehensive security management plan. They engaged a nationally known consultant team to: assess the needs and strengths of current systems, facilities, processes, and operations; analyze information and conditions affecting safety and security; and improve courthouse security through the development and implementation of short, medium, and long-range strategic plans. Working closely with Chippewa County officials and staff over a 9-month period, the consultants have developed the foundation for integrating security into organizational culture and values.

An Integrated Security Plan (ISP) looks at all aspects of County operations to provide for an effective and sustainable security plan; a safe work place and open access to County government. The Chippewa County Integrated Security Plan focuses on People, Operations and Facilities.

The assessment and recommendations utilize security measures of Deterrence, Detection, Delay, and Response. It was determined early on in the planning process that the Courthouse is the "people's building". In doing so, we would blend the public's access and security into one cohesive and fiscally pragmatic plan. That being said, the subject of having only one access point to the Courthouse was eliminated.

The format used in the Security Plan was to Assess, Analyze, and Actualize the Plan. Participants included individuals from diverse disciplines and user group areas. The process used to develop the plan, allowed for education and understanding of the common threads and terminology used for security, i.e. "Themes", growth and understanding on how to apply best practices, balancing the cultural value of an open society, and awareness that small changes can have huge payoffs/benefits to ensure a safe and secure facility and community.

The Security Plan also included an in depth Information Technology Security Management review. The fundamental purpose of information technology security assessment planning is to ensure the confidentiality, integrity, and reliable availability of information and data, and to define, develop, and document information management policies and procedures that support the mission of Chippewa County government. The Security Plan recommendations include the development of written information security policies and procedures that will ultimately represent the foundation for Chippewa County's information security practices. Information management security policies will serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

From the start, the goal was to develop a comprehensive security management plan with action steps the County can implement to improve security and safety both on and off campus.

The initial Phase I recommendations will utilize \$200,000 authorized for security improvements in the 2013 budget. This initial funding will be utilized by the Planning Implementation Team to develop and implement Phase I recommendations. The priority recommendations will focus on security measures for the courts, training for our employees and the development of security policies for the county.

Page 2

Below you will find the Media version of the adopted plan. It outlines the process, methods, recommendations, and the next steps the County can utilize to implement the Integrated Security Plan.

By adopting the Security Plan the Chippewa County Board of Supervisors demonstrated their commitment and leadership to providing a safe and secure environment for the citizens of Chippewa County and County employees.

Please feel free to contact me if you have additional questions.

Sincerely,

A handwritten signature in blue ink, reading "Frank R. Pascarella". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Frank R. Pascarella
County Administrator



Government Campus

Integrated Security Plan

Chippewa County, Wisconsin

Adopted June 11, 2013
Chippewa County Board of Supervisors
Chippewa Falls, Wisconsin

Government Campus
Integrated Security Plan
Chippewa County, Wisconsin
2013

***“Protecting Access to Open Local Government Services;
Dedicated to Public Safety, and to Community Wellness”***

Kenneth Ray – Rod Miller – Mark Purevich
Project Consultants



4200 Woodhaven Court / PO Box 1481 Ashland, KY
606-694-3031 - ken@rjsjusticeservices.com
“Assess – Analyze – Actualize”

Acknowledgements

Chippewa County, WI Government Campus Integrated Security Plan

Chippewa County Board of Supervisors for their commitment to providing a safe and secure environment for the Citizens of Chippewa County and County Employees.

Chippewa County departments and employees who responded to surveys, requests for information and gave of their time to ensure a successful implementation of the Security Plan.

A special thank you to the following individuals who served on the security planning project and gave of their time and talents during the development of the Chippewa County Integrated Security Plan:

Circuit Court Judge - Steven Cray
Clerk of Courts - Karen Hepfler
District Attorney - Steven Gibbs
County Board Supervisor - Jared Zwiefelhofer
Sheriff - James Kowalczyk
District Attorney Office Manager - Diane Lesniewski
Jail Captain - Art Crews
Register of Deeds - Marge Geissler
Child Support Director - Denise Shervey
Assistant Director Public Health - Debra Odden
Human Services Children With Differing Abilities Manager - Tim Easker
Highway Department Shop Superintendent - Paul Mohr
Treasurer - Patricia Schimmel
Human Resources Director - Malayna Halvorson Maes
Information Technology Director - Christi Haun
Facilities and Parks Director - Larry Ritzinger
Risk/Purchasing Manager - Connie Goss
County Administrator - Frank Pascarella

Executive Summary

Chippewa County, WI Government Campus Integrated Security Plan

The following summary provides an overview of the Chippewa County Integrated Security Plan from start-up to recommendations. It is a primer intended to provide the understanding about the methods and processes involved in developing the plan. An extensive and more detailed description of project planning, goals and objectives, and purposes is provided in the Introduction Section of this document. Finally, lengthy and detailed descriptions of vulnerability assessment findings and security recommendations are provided in the Assessment and Recommendation section.

The report was intentionally formatted for ease of use and implementation. This project and plan was initiated by Chippewa County officials to integrate existing and improved security on behalf of the citizens and staff while maintaining a healthy balance between community values and good protection. To this end, county officials and leadership reiterated specific commitments as a framework from which to guide the project through completion and implementation. These commitments include:

- Commitment to a community culture that enjoys a positive courthouse environment
- Commitment to securing open and transparent county government
- Commitment to protecting public access and use of government services and facilities
- Commitment to providing a safe and secure environment for constituents, officials, and staff
- Commitment to continued and ongoing security planning and management
- Commitment to current and future security options and measures

In 2012, Chippewa County officials began an initiative to improve safety and security and to develop a comprehensive security management plan. They engaged a nationally known consultant team to: assess needs and strengths of current systems, facilities, processes, and operations; analyze information and conditions affecting safety and security; and improve courthouse security through the development and implementation of short, medium, and long-range strategic plans. Working closely with Chippewa County officials and staff over a 9-month period, the consultants have developed the foundation for integrating security into organizational culture and values. The project was implemented in four phases.

- Phase 1: Project Start-Up - Develop a Mutual Understanding of Expectations
- Phase 2: Assessment – Comprehensive Inventory of Current and Desired Conditions
- Phase 3: Analysis of Data and Information – Current, Mid and Long-term Impacts
- Phase 4: Actualization – The Action Plan

Goals and Objectives. Security was assessed in terms of: (1) public and private property; (2) personal safety; and (3) integrity of government process. Four primary methods were

identified:¹ Deterrence (preventing threats); Detection (identifying a threat when it is being implemented); Delay (slowing down a threat event to enable timely retreat and/or response; and Response (neutralizing the threat).

Throughout the process, Chippewa County has embraced these concepts. Deterrence, Detection, Delay and Response are the cornerstone of successful security, and aide in the actualization of improved security.

Threats. Managing risk-- improving safety and security-- begins with identifying the threats that are of concern and the exploring the dynamics associated with those threats. Most of the recommended changes in this plan are designed to *reduce the likelihood of success* for threats that are attempted. Threats have been identified and described in terms of: target (may be human or object), intended outcome, motive, means (methods), actors (persons involved), including but not limited to perpetrators, victims, obstacles and bystanders.

Some of the most serious threats identified by officials and employees involved inflicting injury or even death on officials, participants in court proceedings and/or others, including violence between parties, active shooter situation, verbal abuse, threatening, mentally ill persons, persons under the influence of drugs or alcohol, defendants who are jail inmates, riot, major disturbance, and employees or former employees who are angry about their treatment. Many employees expressed concerns about the *ease with which weapons, especially guns, could be brought into the building* and even into a courtroom. Just about every location in the courthouse and on the campus was identified by one or more employee.

Deterrence. In Chippewa County, there is very little effective deterrence in place. One employee stated that there is “no apparent security” in the building or the courts. Deterrence is described in two categories in the plan: *Physical or Facility Deterrence*, accomplished by physical features such as walls, doors, locks, and cameras, and; *Operational Deterrence*, accomplished by people and practices, presence of security personnel, employees.

Detection. Detection occurs when a threat is discovered, hopefully before it is completed. Sometimes detection is accomplished by a person at the scene. When this person is qualified and authorized to act (a deputy, security officer or similar security personnel) detection brings immediate response.

In the courthouse, on campus and in the field, *detection* of the varied threats that are of concern depends more on people than technology. Unfortunately, this means that detection will often occur when the threat is being completed, rather than deterring the action or detecting a weapon that might later be employed to implement a threat. Someone might witness the event, or someone might hear something that raises concerns.

¹ As the project progressed, a fourth method, “delay” was added (slowing down the steps in a threat scenario, increasing the probability of detection and providing more time for the response to arrive)

In the *court areas* on the second floor, persons who might detect a threat include county employees, other professionals involved with the court process (lawyers, clerks, court reporters, witnesses, who are frequently law enforcement officials), parties to court proceedings (plaintiffs, witnesses, defendants' family and friends, persons in the building for non-court purposes). The situation in the court areas is similar to most other areas in the courthouse: no security personnel in the building; pull cords located at workstations and usually concealed from view; and telephones located at workstations not in public areas or corridors.

Delay. "Delay" refers to physical and operational features that increase the time it takes to implement a threat event in the form of: physical barriers (locked doors, distance to target) and "steps" such as security screening, additional checkpoints along the route. Some delay features come into play before a threat is completed, such as passing through security screening or waiting for a door to an office suite to be opened from the inside. Some delays happen after the threat has been implemented, such as impeding a thief's exit from the building.

Delays provide more opportunity for detection-- before or after the fact-- and often provide time for a response force to "catch up" with a threat sequence. Delays often apply to responders as well as perpetrators. The same number of locked doors that a perpetrator must pass through will slow down the response as well.

Physical delays, such as staff entrances that require card access, are often "neutralized" by staff practices. The consultants found many instances in which doors that were to be closed and locked according to policy, were not in practice. A consistent theme in the narratives for each department or agency is that "delay is limited."

Response. Response is what happens after a threat has been identified. Ideally, response is swift and effective enough to stop the threat from being implemented. In Chippewa County that is rarely the case.

Response Force. The county has not created or identified a formal "response force" that is authorized and empowered to deal with threats. The Sheriff's Office is the current response force. The pull cords in the courthouse are monitored in the communications center (dispatch), and identification is aided by cameras and, when used, the telephone duress setting.

When dispatch is notified of a threat, a radio call asks for sheriff's employees who are available to respond by running to the courthouse. The sheriff and his staff make every effort to help in such situations, but there are times when no one is available to respond. When this happens, dispatch contacts the Chippewa Falls Police Department and asks for assistance.

If sheriff's personnel are available, a response force might arrive on the scene in the courthouse within two or three minutes. If they are not available, the response may take five minutes or more, depending on the location and availability of local police officers and sheriff's personnel who are on the road.

The response may be faster if there is a deputy or police officer already in the building, which is the case on Monday mornings when inmates are in the courthouse, or when these professionals are involved with court proceedings as witnesses or in other roles.

Security is not convenient

The process to Assess, Analyze, and Actualize the Plan included multiple individuals from diverse disciplines and user group areas. The process used to develop the plan, allowed for education and understanding of the common threads and terminology used for security, i.e. "Themes", growth and understanding on how to apply best practices, balancing the cultural value of an open society, and awareness that small changes can have huge payoffs/benefits to ensure a safe and secure facility and community.

Recommendations. Numerous specific recommendations are offered in the department specific narratives. These have been transposed into an Excel Worksheet Matrix that will aid county officials in their efforts to improve security. The Matrix is a composite list of all the findings and corrective actions to be considered.

Several themes emerged as the plan was being developed:

- Increase awareness
- Build on existing systems
- Expand appropriate use of technology (but not a *substitute* for staff)
- Harden physical delay elements
- Develop "protection in-depth"
- Increase employee control
- Improve communications
- Increase accountability
- Expand training
- Improve performance and test performance periodically

Several sets of recommendations apply to more than one department, to the entire facility, or to the campus. These include:

- Create a 4-Level System of Alert/Alarm (Detection, Response)
- Improve Existing Duress Alarm System (Detection, Response)
- Adjust, Network, Add Cameras (Deterrence, Detection, Response)
- Performance Improvement (Detection, Delay, Response)
- Quality Improvement (Deterrence, Detection, Delay Response)
- Eventually Secure All Primary Entries into Suites (Delay)
- "Harden" Physical Delay Features (Delay)
- Provide Security Staff (in Phases if Necessary) (Deter, Detect, Delay, Response)
- Create Single Public Entry (Deterrence, Detection, Delay)

It is important to note that Security is everyone's responsibility. Security is not convenient. The plan process review developed the understanding and knowledge of those involved regarding security and what an effective security plan should look like/be. It was a collaborative effort and required a lot of hands on activity and work by county staff. It was not your typical "turn key" consultant report, but rather a self-determined and ownership plan that Chippewa County can use as the road map to provide for a safe and secure Government campus and community.

Total Lock-Down Single Point of Entry

Finally, and in keeping with the aforementioned commitments, county officials and staff engaged the important and difficult issue of creating a single public entry point that mandates securing all other building entrances. Although there is strong consensus among all that a facility total "lock down" may produce the greatest security benefits, it is the least cost-effective option, and was determined via the Campus Vulnerability Assessment training that not even a total lockdown is impenetrable.

The imperfect security benefits resulting from a single entrance were considered less valuable when more cost effective and less intrusive alternatives were considered. Adding the importance of the county's commitments to community culture and values to this equation led to the decision to not focus security planning efforts and resources around creating a single point of entry into the courthouse.

SECTION I: *Introduction, Overview & Recommendations*

Chippewa County, WI Government Campus Integrated Security Plan

Providing safe and secure working conditions for county employees, local officials and citizens when they are on the county campus is essential. Chippewa County is committed and desires to maintain safe and secure government services for its citizens, government officials, and employees. Citizens expect safe and secure access to government officials and services. The county courthouse is a symbol of citizen access to, and participation in, local government.

Keeping all Chippewa County facilities and government processes safe and secure without sacrificing the quality of life is especially challenging. It begins with identifying and understanding the evolving threats. It requires:

- Security awareness
- Policies and procedures
- Initial and ongoing training
- Evaluation and improvement

In 2012, Chippewa County officials began an initiative to improve safety and security and to develop a comprehensive security management plan. They engaged a nationally known consultant team, headed by Kenneth A. Ray Justice Services (RJS) to:

1. Assess needs and strengths of current systems, facilities, processes, and operations
2. Analyze information and conditions affecting safety and security
3. Improve courthouse security through the development and implementation of short, medium, and long-range strategic plans.

Foundation for Effective Campus Security

Developing and maintaining effective campus security as an ongoing commitment by county leaders, officials, and staff:

- Elected leaders must clearly and consistently signal this commitment by—
 - Enacting public policy
 - Dedicating adequate resources to develop solid security plans and to sustain plan implementation efforts.
- Appointed officials, such as department heads, must—
 - Diligently carry out policy
 - Responsibly target budget appropriations
 - Ensure that campus security is integrated into organizational culture and values

Effective leadership is required to develop and maintain effective security. Leaders must be:

- Competent
- Collaborative
- Committed
- Consistent in their efforts to—
 - Secure staff ownership
 - Direct staff through accurate job descriptions
 - Support consistent practices with ongoing supervision

Working closely with Chippewa County officials and staff over a 9-month period, the consultants have developed the foundation for integrating security into organizational culture and values.

Goals and Measures

At the beginning of the project, the consultants described the overall goals for the project, identifying three primary areas for which security will be assessed²:

1. Public and Private Property
2. Personal Safety
3. Integrity of Government Process

Three primary methods were identified³:

- Deterrence (preventing threats)
- Detection (identifying a threat when it is being implemented)
- Response (neutralizing the threat)

Objectives were identified, as shown in Figure 001.

² The complete document of Security Planning Goals and Measures can be found in the appendices.

³ As the project progressed, a fourth method, “delay” was added (slowing down the steps in a threat scenario, increasing the probability of detection and providing more time for the response for to arrive)

Figure 001: Primary and Secondary Goals, Methods

SECURITY MATRIX: GOALS		PRIMARY GOALS		
<div style="border: 1px solid black; padding: 5px; text-align: center;"> GOALS → ↓ </div>		PROVIDE A SECURE CAMPUS WITH RESPECT TO:		
		Public & Private Property	Personal Safety	Integrity of Government Process
SECONDARY GOALS	PROVIDE A SECURE CAMPUS BY MEANS OF:	DETERRENCE Prevent and discourage potential events jeopardizing public and private property	Prevent and discourage potential events jeopardizing personal safety	Prevent and discourage potential events jeopardizing integrity of government process
	DETECTION Discover particular undeterred events jeopardizing public and private property	Discover particular undeterred events jeopardizing personal safety	Discover particular undeterred events jeopardizing integrity of government process	
	RESPONSE Take action with respect to events jeopardizing public and private property	Take action with respect to events jeopardizing personal safety	Take action with respect to events jeopardizing integrity of government process	

The consultants went on to identify objectives associated with each of the three primary areas of concern (Public and Private Property, Personal Safety and Integrity of Government Process), as shown in Figure 002, and accomplished by means of Deterrence, Detection and Response.

Figure 002: Objectives

SECURITY MATRIX: OBJECTIVES		PRIMARY GOALS			
<div style="text-align: center; border: 1px solid black; padding: 10px;"> GOALS → ↓ </div>		PROVIDE A SECURE CAMPUS WITH RESPECT TO:			
		Public & Private Property	Personal Safety	Integrity of Government Process	
SECONDARY GOALS	PROVIDE A SECURE CAMPUS BY MEANS OF:	COROLLARY OBJECTIVES			
		DETERRENCE	Vandalism	Events/Situations Jeopardizing Life Safety	General Decorum/Order Incidents
		DETECTION	Theft of Public Property	Natural Disasters/Other Emergencies	Participant Contact Incidents
		RESPONSE	Destruction/Theft of Public Records	Confrontations/Assaults	Incidents Jeopardizing Jury
		Theft of Private Property	Prisoner Escape	Incidents Jeopardizing Tax Collections, Voting, Trials, Hearings, Official and Unofficial Meetings	
			Incidents Involving Weapons		
			Incidents Involving Explosives		
			Hostage/Terrorist Situations	Alteration/Loss of Evidence	

The objectives provided a preview of the range of threats for which county officials had concerns. For example, *property* concerns included vandalism, theft, and destruction. Similarly, *process* concerns included disruption and interference. Response to these threats can be accomplished by Deterrence, Detection, and Response.

Method and Process

The project was implemented in four phases:

- Phase 1: Project Start-Up - Develop a Mutual Understanding of Expectations
- Phase 2: Assessment – Comprehensive Inventory of Current and Desired Conditions
- Phase 3: Analysis of Data and Information – Current, Mid and Long-term Impacts
- Phase 4: Actualization – The Action Plan

Phase 1: Project Start-Up. During this phase, the foundation was established for the following months of work. Working with local officials and employees the consultants:

- Determined expected organization involvement
- Established primary team members
- Clarified project communications
- Estimated required and optional levels of organizational involvement
- Explored potential social, economic, and political influences on the project and its success
- Clarified and attempted to resolve issues of specific concern, and
- Estimated project timelines

Although short in duration, this phase laid the groundwork for the rest of the project.

Cornerstones

At project start-up, Frank Pascarella, County Administrator and Connie Goss, County Risk/Purchasing Manager, in collaboration with project consultants, identified three fundamental foundations from which to build plan development, implementation, and ongoing security management. These cornerstones included:

- Project and Plan Legitimacy
- Project and Plan Implementation and Management
- Leadership Commitment and Readiness

Project and Plan Legitimacy

Any initiative of this nature requires legitimacy. The mere understanding about the importance of government campus security does not provide an adequate foundation for justifying use of scarce public resources for the intended purposes. Development of an integrated campus security plan is only the first step to create safer and more secure government service delivery system; the ultimate objective is to implement the plan via an ongoing investment of time and financial resources. To this end, both the planning project and plan implementation require the full commitment from elected policy makers and leaders.

Planning and plan implementation legitimacy was established early on by the Chippewa County Board of Supervisors through unanimous support and adoption of the following resolution. This resolution clearly evidences the legitimacy for campus security planning and plan implementation while establishing the necessary structural and leadership requirements⁴.

⁴ The signed official resolution is on file with the Chippewa County Administrator.

**RESOLUTION 08-12 TO ESTABLISH A CHIPPEWA COUNTY
GOVERNMENT CAMPUS INTEGRATED SECURITY PLANNING PROJECT**

WHEREAS, effective and efficient delivery of local government services is fundamental to quality of life for the citizens and employees of Chippewa County, Wisconsin; and

WHEREAS, such service delivery fundamentally relies on providing safe and secure county campus environments for Chippewa County citizens and employees to access and conduct services; and

WHEREAS, Chippewa County acknowledges its obligation and duty to provide safe and secure county campus environments; and

WHEREAS, Chippewa County believes that the development and implementation of a comprehensive security plan that guides methods for deterring, detecting, and responding to security risks and threats and that applies the principles of Integrated Security Planning that focus on people, facilities, infrastructure, and daily operations is a legitimate action for meeting its obligation and duty to provide safety and security to county campus environments; and

WHEREAS, Chippewa County also acknowledges the importance and value of Wisconsin Supreme Court Rule 68 (SCR 68), Court Security, Facilities, and Staffing in assisting the county in meeting these obligations and duties; and

WHEREAS, the Chippewa County Board of Supervisors directs and assigns the responsibility and authority to the Chippewa County Administrator to develop, implement, and administer a comprehensive integrated government campus security plan; and

WHEREAS, the Chippewa County Board of Supervisors authorized funding for the development of a comprehensive and integrated Chippewa County Government Campus Integrated Security Planning Project in the 2012 budget.

NOW, THEREFORE BE IT RESOLVED, that the Chippewa County Board of Supervisors does hereby endorse and adopt the attached Integrated Security Planning Project Structural Chart that delineates roles and responsibilities for project oversight, policy and procedure development, and collaboration and communication among stakeholders that will maintain transparency and inclusion throughout the lifecycle of the project and through plan implementation; and

BE IT FURTHER RESOLVED that the County Administrator shall bring back to the County Board a final Integrated Security Plan for adoption that will allow Chippewa County to reach the goal of providing a safe and secure county campus for Chippewa County citizens and employees.

Structure for the Integrated Security Plan, Implementation and Management

As stated in the above resolution, “*Chippewa County believes that the development and implementation of a comprehensive security plan that guides methods for deterring, detecting, and responding to security risks and threats and that applies the principles of Integrated Security Planning that focus on people, facilities, infrastructure, and daily operations is a legitimate action for meeting its obligation and duty to provide safety and security to county campus environments...Chippewa County Board of Supervisors directs and assigns the responsibility and authority to the Chippewa County Administrator to develop, implement, and administer a comprehensive integrated government campus security plan...Chippewa County Board of Supervisors does hereby endorse and adopt the attached Integrated Security Planning Project Structural Chart that delineates roles and responsibilities for project oversight, policy and procedure development, and collaboration and communication among stakeholders that will maintain transparency and inclusion throughout the lifecycle of the project and through plan implementation.*”

This statement sets clear expectations for structuring the planning process and plan implementation by designating ultimate responsibility to the County Administrator.

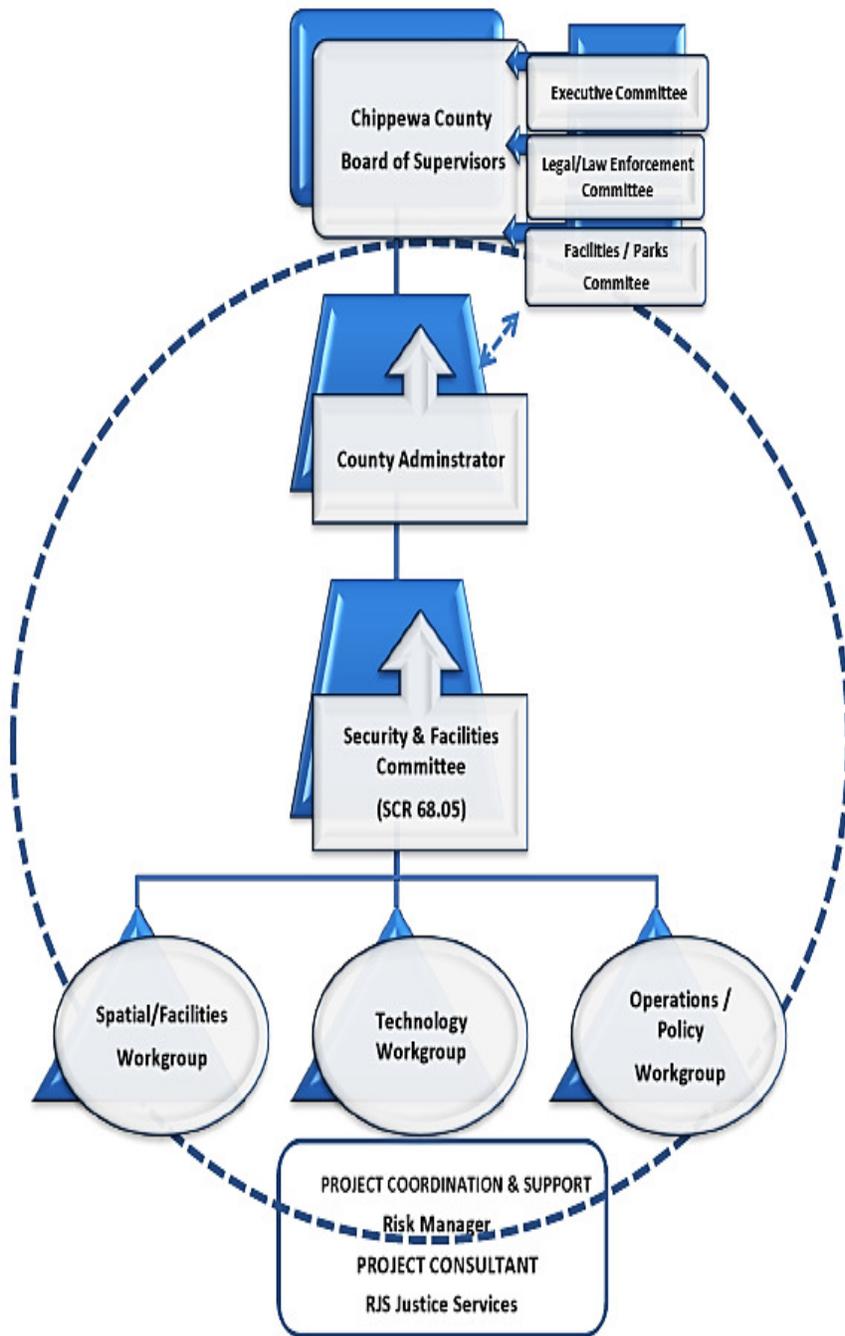
The Board of Supervisors further endorsed the requirement for internal collaboration and transparency. The *Integrated Security Planning Project Structural Chart that delineates roles and responsibilities for project oversight, policy and procedure development, and collaboration and communication among stakeholders that will maintain transparency and inclusion throughout the lifecycle of the project and through plan implementation.*

Project structure was designed to ensure successful actualization of security planning and plan implementation while facilitating desired outcomes using three specific mechanisms:

- Establish systematic collaboration and communication with and among stakeholders.
- Maintain transparency and inclusion throughout the life cycle of project and into plan implementation.
- Ensure efficient and adequately organized planning methods and processes for sustainable, positive momentum.

Figure 003 below shows the structure support chart reviewed and adopted by the Board. The County Administrator and project coordinator closely monitored project structure and these supporting mechanisms from project start-up through plan completion.

Figure 003: Integrated Security Planning Project Structural Chart



**CHIPPEWA COUNTY,
WISCONSIN**

**2012 Government Campus
Integrated Security Planning
Project Structural Chart**

This chart is intended to provide structure for the successful actualization of the Chippewa County Government Campus Integrated Security Plan.

Project structure is designed to facilitate project outcomes by:

- 1 **ESTABLISHING** systematic collaboration and communication among stakeholders.
- 2 **MAINTAINING** transparency and inclusion throughout the lifecycle of the project and in to Plan implementation.
- 3 **ENSURING** efficient and adequately organized planning methods and processes for sustainable, positive momentum.

Leadership Commitment and Readiness

Strong consensus of support and need among county leaders at all levels vividly evidenced project commitment and readiness. To their credit, the county administrator and project coordinator requested an assessment of leadership readiness in an effort to quantify salient aspects of leadership readiness and the capacity of organization support for leadership's commitment. A survey of the entire organization using the Leadership Performance Expectations Inventory – Revised (LPEI-R) accomplished this objective.⁵

The LPEI-R is a tool used to inventory local government employee (leadership and line-staff) perceptions about the importance of specific leadership traits. Seven (7) trait categories consisting of sixty-three (63) leadership traits were assessed by asking each employee to rate how important each trait is to them personally and how important they (the employee) thinks the trait is to their leaders.

LPEI-R Trait Categories Assessed

1. Importance of Leadership Integrity
2. Importance of Basic Leadership Proficiency
3. Importance of Effective Leadership Communications
4. Importance of Leadership Management of Resources
5. Importance of Team Work
6. Importance of Customer Service
7. Importance of Leadership Accountability

Comparing the results provides a measure by which to understand what employees expect from their leaders and the extent to which leaders are meeting those expectations relative to the levels of importance the employees indicated on the assessment tool. Over 270 employees (leaders and line-staff) completed assessment surveys. A cursory aggregate analysis was performed to determine trait importance to employees and the degree to which leaders, according to the employees, were meeting assessed leadership performance expectations.

Assessment results clearly suggest that employees and leaders agree that all 63 traits are important to them personally as well as being important to leaders. This consensus shows that what is important to employees is also important to leaders and that leaders, in general have, done a good job leading their respective staff in the day-to-day delivery of government services, as well as in garnering organizational support for successful planning and implementation of change. Overall, the results strongly evidence the presence of mutual support within the organization. The results not only illustrate solid leadership readiness for security planning and plan implementation, but also solid organizational support for the project and beyond.

Phases 2 & 3: Assessment and Analysis. These phases required the most time to implement. Assessment involved a comprehensive evaluation of policy, practices, facilities, operations, methods, technology, resources, perceptions, strengths and needs, historical and trend data and information, existing site and facility plans, and more. This provided the consultants with a clear understanding of the physical, technological, systems, and operational and environments in which Chippewa County

⁵ LPEI-R is a proprietary organizational assessment instrument developed and owned by RJS.

delivers government services. Areas of assessment involved examining a variety of information and data, including:

- Strengths, vulnerabilities, opportunities
- Internal and external environments/spaces
- Human and technology system functions
- Operations
- Staffing
- Policy and procedure
- Processes and requirements and security measures
- Existing site and facility master plans
- Criminal justice services and trends
- County facility use, structural design, layout, proximities, adjacencies, systems
- Security policy and practices
- Staff perception of security and risk
- Community expectations and concerns about change

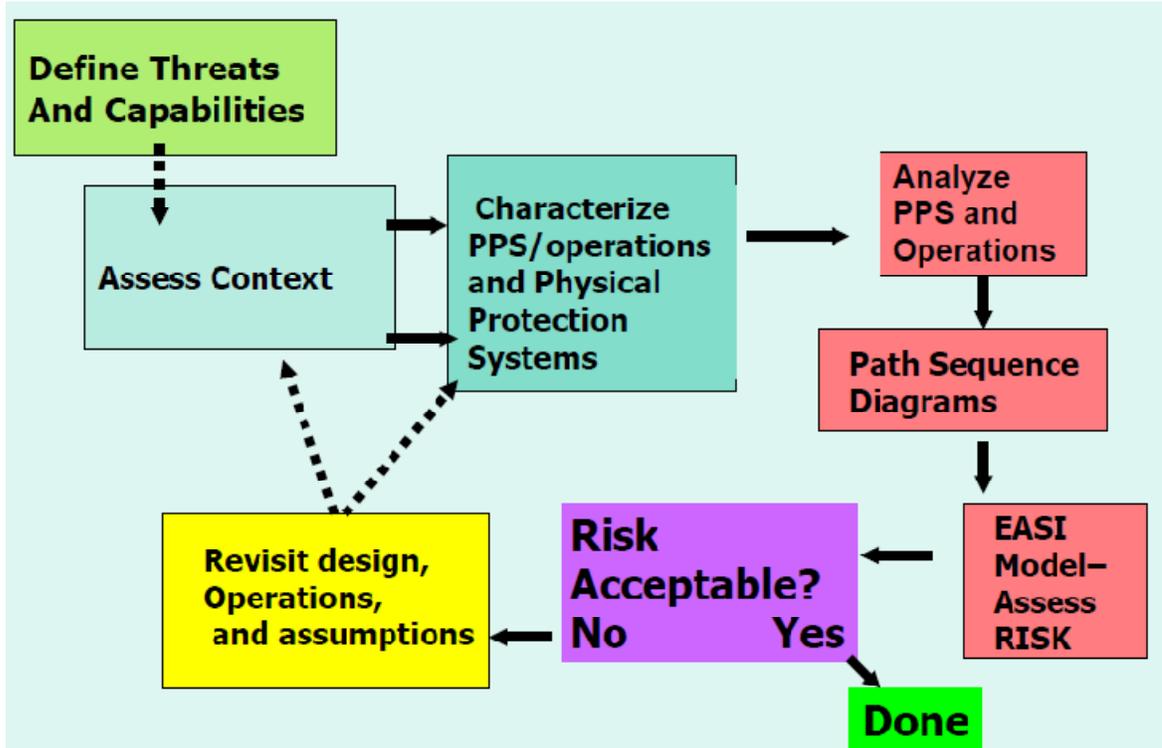
A critical activity during the assessment phase assessed security vulnerability. RJS conducted a vulnerability assessment as a key element to maximizing stakeholder involvement and ultimate security planning.

Vulnerability Assessment

The consultants adapted an innovative “vulnerability assessment” (VA) methodology for use as a central component of this project. The VA process and tools were developed by Sandia National Laboratories for the U.S Department of Defense and the Atomic Energy Commission.

The vulnerability assessment process is a central component of the overall Risk Evaluation Process. In Figure 004 below, the three components on the right side of the diagram—Analyze PPS and Operations, Path Sequence Diagrams, and EASI- modeling and assessing risk.

Figure 004: Risk Evaluation Process – Security Physical Protection Systems (PPS)



When first developed, the VA process focused on asset protection, such as protecting weapons or nuclear material from theft. The U.S. Department of Justice adapted the VA process for use in prisons and jails, RJS and the Chippewa County team was the first to use it in the context of court security. Vulnerability assessment is the ultimate tool for assessing courthouse security.

A core group of officials and employees were selected to participate in the VA training. Participants included:

- *Circuit Court Judge - Steven Cray*
- *Clerk of Courts - Karen Hepfler*
- *District Attorney - Steven Gibbs*
- *County Board Supervisor - Jared Zwiefelhofer*
- *Sheriff - James Kowalczyk*
- *District Attorney Office Manager - Diane Lesniewski*
- *Jail Captain - Art Crews*
- *Register of Deeds - Marge Geissler*
- *Child Support Director - Denise Shervey*
- *Assistant Director Public Health - Debra Odden*
- *Human Services Children With Differing Abilities Manager- Tim Easker*
- *Highway Department Shop Superintendent - Paul Mohr*
- *Treasurer - Patricia Schimmel*
- *Human Resources Director - Malayna Halvorson Maes*

- *Information Technology Director - Christi Haun*
- *Facilities and Parks Director - Larry Ritzinger*
- *Risk/Purchasing Manager - Connie Goss*
- *County Administrator - Frank Pascarella*

The training was implemented in a series of three 2-day sessions during October and November 2012. Much of the training involved hands-on learning as teams implemented assignments in various areas of the campus. In the final stages of the training, participants developed specific threat scenarios and used the EASI⁶ program to calculate the probabilities of threat success.

Everyone involved with the project, especially the core team members, are now well versed in the vulnerability assessment process. The findings are not theoretical, but rather tested on site through team member observations and testing (assignments between site visits). The process heightens everyone's level of acuity re: security (facility, technology, operations).

Phase 4. Plan Actualization. Actualization and implementation of the security plan started from the outset, as officials and employees increased their awareness of security and articulated threats. Participants in the VA training emerged with new perspectives and skills that they brought in to the analysis. During the course of the project, some policies and practices were changed in light of heightened awareness of security.

All recommendations have been transposed into an Excel-based format that identifies the form and function of each proposed improvement, as suggested in Figure 005.

⁶ EASI- Estimate of Adversarial Sequence Interruption, developed by Sandia National Laboratories. User entered probabilities of detection an amount of delay for each step in a scenario. When the response time is entered, the EASI programs calculates the probability that the scenario will be interrupted before the threat has been carried out.

Figure 005: Form and Function

Form	Function
Facilities	Deter
Technology	Detect
	Delay
Operations	Response

Plan actualization involves any or all of the following, as determined by the project team:

- Plan
- Direct
- Train
- Model
- Reinforce
- Test
- Refine

Actualization requires all parties to:

- Think
- Learn
- Prepare
- Practice
- Use

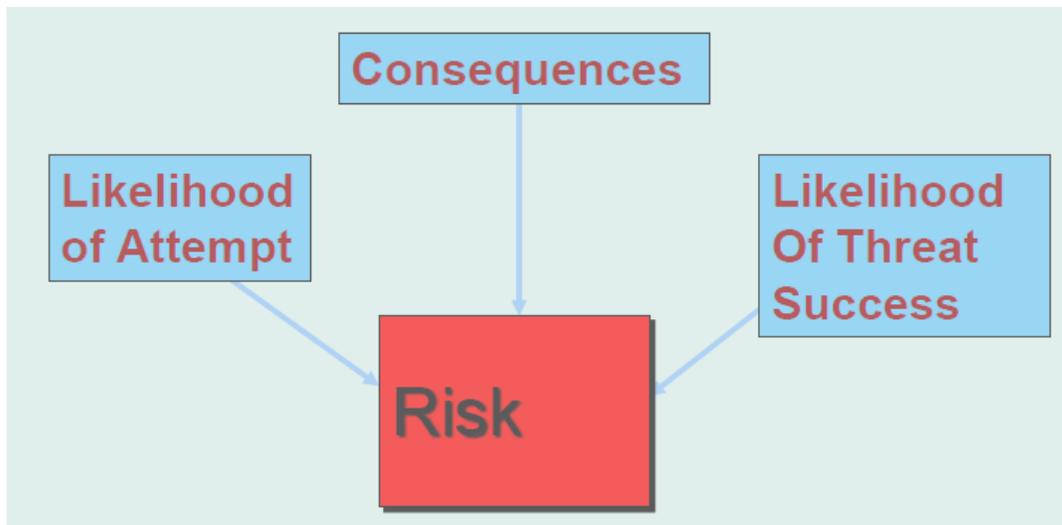
Identifying and Assigning Priority to Risks

As county officials begin to implement elements of this plan, it will be necessary to set priorities regarding the risks that will be addressed first. Three primary considerations will come into play:

- Likelihood a threat will be attempted
- Likelihood that a threat will be successful if attempted
- Consequences if the threat is successfully carried out

Figure 006 illustrates these factors.

Figure 006: Prioritizing Risks



Some threats will have disastrous consequences, such as a bomb detonating in the courthouse, but may have a low likelihood of being attempted. Under current conditions, it is likely that such a threat would be successful if attempted.

Conversely, a verbal assault on an employee by a citizen, while unpleasant, would be considered a lesser consequence. But this type of threat has already been visited on county employees many times, and is likely to be repeated many times in the future. Under current conditions, it is likely that these threats will continue to occur. While many of the recommendations in this plan would reduce the opportunity to implement this threat, it is not possible to eliminate the opportunities.

County officials will need to balance these considerations with the costs associated with proposed improvements and other considerations, such as the effect on employee morale, inconvenience, reduced efficiency, and similar concerns.

Information Technology Plan

Chippewa County, WI Government Campus Integrated Security Plan

Overview

Chippewa County, WI leaders fully embrace the importance of government campus integrated information technology security; this responsible decision is as important as it is timely. The “information age” is a renaissance bringing with it amazing advancements in human connection, technology, business and government operations, public safety and criminal justice, and the horizon of change is not in sight. However, surrounding all advancements remains the increasing, constant, and unrelenting demand to protect our greatest power on earth: readily available access to valuable, valid, and reliable information. Protection information and the technology that maintains and moves it is as important as the purpose of the information. Comprehensive, deliberate, and ongoing information security planning is now more important than ever before in the history of local government information management.

Chippewa County leaders intentionally engaged comprehensive and integrated information security planning in 2012. This work launched from a solid foundation built upon structured and collaborative assessment and evaluation of information management security policies, practices, and environments. County officials together and in collaboration with professional security consultants tackled the arduous task of comprehensive program assessment. The assessment process involved detailed review and re-review of current security conditions. Security strengths and improvement opportunities were identified empirically and through numerous discussions. Assessment findings were collated into priorities and a three-year improvement implementation plan was developed by officials. However, an ambitious list of improvements, county leaders are confident about the importance of chosen priorities, and are unequivocally competent and motivated to accomplish these priorities and beyond.

Purpose

The fundamental purpose of security assessment planning is to assist in ensuring the confidentiality, integrity, and reliable availability of information and data, and to define, develop, and document information management policies and procedures that support the mission of Chippewa County government. Additionally, responsible security assessment and planning assists government officials satisfy their legal and ethical responsibilities with regard to its information technology and management resources.

Well-developed and written information security policies and procedures will ultimately represent the foundation for Chippewa County’s information security practices. Information management security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud, and abuse from occurring, and assist in resolving discrepancies that be accidentally introduced in the operations of county business. When consistently applied via

effective and supportive leadership, these policies and procedures assure that the information assets are protected from a range of threats in order to ensure business continuity and maximize the return on investment of scarce and valuable tax dollars and other investments.

This assessment and planning work is vivid reflection of Chippewa County's commitment to responsible stewardship of sensitive personal information and critical business information, in the acknowledgement of the many threats to information security and the importance of protecting the privacy of the public and staff, safeguarding vital business information, and fulfilling legal obligations. This assessment planning effort will be reviewed and updated periodically to maintain its value and relevancy to its intended purpose.

Conclusions and Next Steps

Strengthening and sustaining campus security is neither convenient or inexpensive. Security improvements will require changes in staff work habits, the environment, technology, and operations. Change, especially change that affects work habits and operational policies, requires careful planning and implementation.

The Government Campus Integrated Security Plan provides general concepts for planning and implementation as well as specific recommendations for improving security via increased measures to Deter, Detect, Delay, and Respond to threats. It is important to note that security planning never fully departs from the "planning" process. Initial and ongoing planning, implementation, and evaluation of plan efficacy and effectiveness is normal.

Effective security management of government facilities and people is a never ending and an ongoing process. This plan was specifically written for these purposes as well as to provide options for selection of security improvements that balance security needs with fiscal realities and community values of open government. The process of plan review included a back and forth review between the consultant and County staff, as the collaborative and ownership effort of the plan creation evolved. The process allowed full participation and self actualization to ensure successful implementation. **It is the County's plan.**

Next Steps

County officials, specifically the county administrator and security project coordinator/risk manager, are now charged with developing a strategic action plan for implementing Plan recommendations. A strategic implementation plan should apply the same concepts and process used in developing the Integrated Security Plan i.e. stakeholder collaboration, prioritization of recommendations according to risks, needs, economics, and community values. The strategic plan should lay a foundation for stakeholder involvement, decision-making, and process methods. This foundation should remain intact throughout the life-cycle of the security program.

Plan implementation should use a phased approach over a 2-5 year period. Each phase would build upon the previous phase while continuing to enhance security. The following three elements are critical to the survival of the security program and should remain consistent:

1. Commitment – Annual budget lines for the security program, or create a Security Program Budget as a stand-alone cost center
2. Continuity of Involvement – Maximize processes involved in the development of the Integrated Security Plan (ISP) involving as many of the participants as possible.
3. Quality Management – All security measures implemented should undergo rigorous and periodic quantitative and qualitative evaluation. Specific structure, process, and performance outcome metrics must be developed to ensure that security measures are meeting their intended outcomes.

Plan Implementation, Recommendations & Estimated Costs

Phase I implementation of the plan can begin in 2013. The County Board allocated funding in the 2013 budget for Security. It is recommended that Phase I include implementation of security measures that respond to areas of greatest risk and need, as well as to begin to lay in the “back-bone” for subsequent phases.

Phase II implementation will continue into year 2-5 and ongoing. This phased approach allows for planning, budgeting, and allocating appropriate resources to evaluate and implement the proposed recommendations that are indicated on the Planning Matrix. Items to consider during Phase II include staffing, facility space and use, enhanced environmental controls and ongoing policy and procedure development.

The county administrator should evaluate and recommend options to the County Board for security implementation funding that will include the components of property, personal safety, and integrity of government operations.

The County Administrator should establish a security implementation team to assist with the review of the recommendations and development of a planned approach for implementation based on organizational capacity.

The implementation team should utilize the Planning Matrix to assist in the development and funding of these priorities. Utilizing the Matrix based on critical needs assessment of the listed security recommendations and available funding over a period of several years. Emphasis should be given to the support and enhancement that Technology provides to gain efficiencies and provide for cost effective security solutions.

The following recommendations apply the principals of Detection, Deterrence, Delay, and Response and should be considered for Phase I implementation:

Phase I Estimated Cost:

Security Measure	Estimated Cost
A&E Work	\$50,000
IP Conversion of existing Cameras	\$25,000
Additional IP cameras	\$32,000
Card Locks (cost range)	\$18,000 -\$60,000
Policies & Procedures, Technical Assistance, Training	\$49,000
2013 Estimated Phase I Cost	\$209,000 - \$269,000

- Judicial areas (2nd) floor should be considered top priority for implementation of specific recommendations.
- Additionally, the county should engage qualified A&E services to assess and develop design plans for structural security improvements in those areas.
- A&E Cost Estimate: \$50,000

Under Phase, I Deterrence **and Detection** apply to the following Improvements:

The existing camera technology should be converted over to IP technology. It is assumed, based on information previously provided by county officials that all existing cameras have digital capabilities requiring no cost for analogue converters. Conversion to IP will require involvement by county IT officials because additional bandwidth and digital storage may be required.

Conversion Cost Estimate: \$25,000

Additional internal cameras should be added to higher risk areas to allow monitoring of lobby areas as discussed in this plan. Wireless cameras should be considered due to their cost effectiveness. This should include following areas with an Estimated Cost: \$32,000

DOA reception areas	1-3	Housing Authority main reception	1
Treasure reception	1	Land Records/ Surveyor reception	1
Clerk reception area	1	Planning and Zoning	1
Register of Deeds	1	Facilities and Parks reception – 1	1
Public Health reception areas	3	UW Extension reception – 1	1
ADRC/CMHRC reception	1	Highway Department main entrance – 1	1
Courts - TBD	TBD	Land Conservation and Forest	1
District attorney reception area	1	Management reception – 1	2
Clerk of Court reception	1	Assembly Room (both sides) -2	1
Child Support reception	1	Highway Department reception – 1	1
Juvenile Intake and Probate reception	1		
Board of Supervisor meeting room	1		
DHS reception	1	Total Cameras: 27	

Phase I Deterrence **and Delay** Improvements include:

Replace mechanical locks at key access points with card locks:

Estimate locks required: 30

Estimated Cost: \$18,000 - \$60,000

Begin Integrated security policy and policy review, revision, develops implementation,& training; Plan implementation technical assistance and support; Leadership development and security training initial phases. Estimated Cost: \$49,000

Road Map and process for successful implementation

Section II Security Assessment and Recommendations include the department specific narratives and recommendations. It includes the thorough review of the County's Information Technology plan and System Security. All the recommendations from Section II have been converted to the Planning Matrix.

The Integrated Security Plan and Matrix Planning Tool is the roadmap and process that the Chippewa County Board of Supervisors can use for policy and budget decisions, its purpose is to help the County Board provide for a safe and secure community.

Security is not convenient; it takes a commitment and leadership.

We at RJS Consultants thank you for the opportunity to be part of your integrated security plan.