Isabel Hernandez

From: Art Provenghi
Sent: Monday, February 08, 2010 5:18 PM
To: Isabel Hernandez
Cc: Frank Cress
Subject: Contract Review Form KK-10-069-EPSO Interlocal with the UTEP Police Department
Attachments: k10069 Interlocal UTEP PD and EPSO.doc; k10069 SO Non-Disclosure Agreement-UTEP PD.doc; k10069 SO RMS Security Policy-UTEP PD.doc

EL PASO COUNTY LEGAL REVIEW FORM

KK-10-069

Contract Description: Sheriff's Office-Interlocal Agreement with the University of Texas at El Paso (UTEP) Police Department for deployment of the Crime Records Information Management Enterprise System (RMS)

COUNTY ATTORNEY ACTION**

**Requested Amendments/Clarifications: Please list any questions or comments you have regarding the terms of the contract, as well as any specific provisions to which you object, or which you want to have changed.

___X___ Approved as to Form as Submitted
_____ Approved as to Form with Amendments/Modifications/Reservations Noted Below*
_____ Not Approved

*1)

This document has been given legal review by the El Paso County Attorney's Office on behalf of the County of El Paso, its officers, and employees. Said legal review should not be relied upon by any person or entity other than the County of El Paso, its officers, and employees.

Art Provenghi
Assistant County Attorney
Date: February 8, 2010

STATE OF TEXAS)
)
COUNTY OF EL PASO)

INTERLOCAL AGREEMENT

FOR LAW ENFORCEMENT INFORMATION SHARING

This Interlocal Agreement is entered into by El Paso County on behalf of the El Paso County Sheriff's Office ("SO") and University of Texas at El Paso Police Department ("UTEP PD"), also hereinafter referred to as ("Contributing Agency"), for the purpose of deploying the Crime Records Information Management Enterprise System (hereinafter referred to as RMS System).

RECITALS

WHEREAS, the Interlocal Cooperation Act, Sec. 791.001, et seq., Texas Government Code, authorizes local governments to contract with one another to carry out their governmental functions; and

WHEREAS, public safety in the region will be significantly enhanced with sharing of information through the use of the RMS System by participating agencies; and

WHEREAS, the SO and the UTEP PD agree that providing information sharing and services on a regional basis will provide more efficient, effective, and less costly services for both the University of Texas at El Paso and the County of El Paso, thereby serving the public; and

WHEREAS, the SO is the lead participating agency for the RMS System, has a contract with Intergraph Public Safety Inc. to provide a certain number of licenses for the software used in the RMS System and is permitted to allow other law enforcement agencies to use the licenses under its licensing agreement; and

NOW, THEREFORE, in consideration of the mutual promises contained herein, and of other good and valuable consideration, and intending to be bound hereby, the SO and UTEP PD agree as follows:

1. This Interlocal Agreement relates to the participation by the Contributing Agency in the RMS System, where as the Contributing Agency will assume all connectivity cost to interface with the RMS. UTEP PD shall cover all costs associated to connectivity to the RMS. UTEP PD may elect to participate to connect to the RMS through the County Citrix Server System which provides a secure internet access. If UTEP PD elects to connect by means of the Citrix Server, UTEP PD will be required to purchase an appropriate number of concurrent

Citrix Licenses that are agreed upon by the SO. Typically Citrix licenses are acquired in incremental lots of five each.

2. UTEP PD understands that each user shall be entitled to access the RMS System by one open session of RMS at any given time. The SO reserves the right to monitor usage of the RMS and if the Contributing Agency's use exceeds usage of the initial agreed upon access, the SO shall then inform the Contributing Agency in writing that the Contributing Agency shall provide the additional funding to purchase additional licenses and be required to increase funding for the annual maintenance. The SO shall provide a 90 calendar day written notice of the increase to the Contributing Agency to allow time for the Contributing Agency to secure additional funding. On the date that is 90 calendar days from the date of the Sheriff's written notice, this Interlocal Agreement shall automatically be amended to include the additional licenses without further action by the parties. If UTEP PD/Contributing Agency fails to make payment for the additional licenses, the SO, at its option, may suspend service or terminate this Agreement and the right of the Contributing Agency to use the RMS System.

3. The parties understand that the RMS system has been approved by the governing bodies of the County and the City of El Paso and was developed jointly by the Sheriff's Office and the City's Police Department. Any meetings or discussions among parties in designing and implementing the RMS system have been conducted in compliance with this authorization, and any recommendations for changes to the RMS System will be provided to the RMS System Project Manager for presentation to the El Paso Sheriff's Office and the El Paso Police Department.

4. SO will create an "agency" on the RMS for the Contributing Agency's use and allow the Contributing Agency to enter their law enforcement data and enable them to share certain basic criminal justice data among Contributing Agencies for authorized law enforcement purposes only. SO will provide the Contributing Agency with technical assistance for the setup, configuration, and assistance in the operations and processes for UTEP PD to utilize the RMS system. The SO will also assist with initial training to the Contributing Agency officers. Training shall consist of a three day training course on the usage of the RMS system. Contributing Agency shall ensure that only RMS-trained law enforcement personnel shall use and have access to the RMS System.

5. The Contributing Agency will enter their law enforcement incident data, and other criminal justice data as agreed by the SO and the Contributing Agency into the RMS system. The County and City of El Paso have developed an RMS Security Policy. Contributing Agency will follow RMS system policies and procedures for the submission, query, and use of all data. The Contributing Agency will ensure that only authorized persons performing authorized functions have access to the RMS system.

6. The RMS system is designated as a LAW ENFORCEMENT SENSITIVE BUT UNCLASSIFIED system. The Contributing Agency shall ensure that data entered into the RMS system is SENSITIVE BUT UNCLASSIFIED and free of

classified National Security Information.

7. Computer security-related incidents and/or violations, as defined by the RMS Security Policy, must be reported to the SO by the Contributing Agency. The SO reserves the right to suspend services. Procedures for both the Contributing Agency and the SO are outlined in the RMS Security Policy.

8. The Contributing Agency retains sole ownership of and sole responsibility for the information it contributes, including but not limited to, the accuracy of the information. The RMS system clearly creates a separate database for the Contributing Agency's data, segregating its data from other participating agencies on the RMS. Certain data shall be considered "shared data records" that will not be restricted from viewing by any other participating agency, i.e. data in the Names, Locations, Property, and Employees data sets. The Contributing Agency understands the information entered into the RMS remains the sole property of the Contributing Agency and its exclusive control with the exception of data entered in the Names, Locations, Property, and Employees data sets which shall be treated as shared data.

9. The Contributing Agency agrees that the information it contributes can be utilized by the El Paso Police Department Fusion Center for purposes of reporting regional crime statistics and performing crime analysis, field operation, and investigation functions.

10. Each party to this Agreement agrees that it shall have no liability whatsoever for the actions and/or omissions of the other party's employees, officers, or agents, regardless of where the individual's actions and/or omissions occurred. Each party is solely responsible for the actions and/or omissions of its employees, officers, and agents; however, such responsibility is only to the extent permitted by Texas law. Where injury or property damage result from the joint or concurring acts and/or omissions of the parties, any liability shall be shared by each party in accordance with the applicable Texas law, subject to all defenses, including governmental immunity. These provisions are solely for the benefit of the parties hereto and not for the benefit of any person or entity not a party hereto; nor shall any provision hereof be deemed a waiver of any defenses available by law.

11. SO shall have the authority to inspect and audit the equipment records and operation of the Contributing Agency to determine compliance with this agreement, RMS security policy, procedures, and all applicable state and federal laws.

12. SO reserves the right to immediately suspend service to the Contributing Agency when SO determines that this agreement or any applicable state or federal law, rule, or regulation has been violated by the Contributing Agency or an employee of the Contributing Agency. The SO may reinstate the service upon the Sheriff's receipt of satisfactory assurances that such violations have been corrected and measures have been taken to prevent future violations by the Contributing Agency. All costs for service reconnection are the responsibility of the Contributing Agency.

13. Either SO or UTEP PD may upon 30 days written notice discontinue service or participation in the RMS system for convenience. Any cost associated with termination and the movement of the Contributing Agency's data shall be borne by the Contributing Agency.

14. The laws of the State of Texas shall govern all questions and interpretations concerning the validity and construction of this Agreement and the legal relations between the parties and performance under it.

15. The SO and the UTEP PD agree to observe all local, federal and state laws, rules and regulations that in any manner affect or govern the services to be performed under this Agreement and the operation of the sensitive law enforcement information.

16. The parties to this Agreement do not intend for any third party to obtain a right by virtue of this Agreement.

17. Except as set forth in Paragraph 2, any alterations, variations, modifications or waivers of provisions of this Agreement shall only be valid if executed as an amendment to this Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement by the signatures of the duly authorized representative of each on the dates indicated. This agreement is effective upon the last signature date.

ATTEST:

_____
Delia Briones
County Clerk

_____
Date

THE COUNTY OF EL PASO:

By:_____
Hon. Anthony Cobos
County Judge

_____
Date

Chief of Police University of Texas at El Paso

_____
Clifton Walsh, Chief

El Paso County Sheriff

_____
Richard Wiles, Sheriff

RMS Security Policy
El Paso County Sheriffs Department

FINAL
2 January 2007

1 RMS Security Overview

1.1 Purpose

The purpose of the RMS (Record Management System) Security Policy is to ensure that the RMS and the county network and the information stored therein is protected from unauthorized access. The Sheriffs Office (SO) has established this policy to insure security for the RMS, the county network and interconnecting agencies will make every effort to avoid undue hardships on other local agencies. These standards are intended to be applied to every agency connecting to the RMS and county network.

1.2 Executive Summary

The Law Enforcement Automated Records Management System (RMS) also known as the Criminal Records Information Management Enterprise (CRIME) System is an incident based report writing and tracking system. The system was implemented with goal of being a regional concept of data sharing and utilization by criminal justice agencies. The system provides the means to electronically collect, store, and transmit officer field reports, arrest reports, and other associated information and reports utilized by criminal justice agencies. The incorporation of the RMS streamlined operational processes, eliminated redundant entry of information, and standardizes data elements. The system facilitates information sharing and enhances cooperation among local, state, and federal criminal justice agencies.

1.3 Scope

The document outlines responsibilities that agencies will follow to insure security on the RMS, county network, and interconnecting agencies. The Sheriff's Office will be the primary management activity for the implementation and controls established herein. Network infrastructure management assistance shall be provided by the Sheriff's Office technical support infrastructure. The formal assignment of the RMS Program Manager and the RMS Program Leaders are to provide the daily oversight and technical liaison between agencies.

2 Roles and Responsibilities

2.1 RMS Program Manager

The Sheriff's Office as the lead agency for RMS designates the Sheriff's Office IT Manager as the RMS Program Manager.

2.2 RMS Program Manager Responsibilities

The RMS Program Manager (PM) is responsible for establishing and administering an Information Technology (IT) security program throughout the RMS user community. The RMS Project Manager is therefore responsible to set, maintain, and enforce the following:

- Standards for the selection, supervision, and separation of technical personnel who have administrative RMS systems access.
- Policy herein governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network related to the RMS systems, use to process, store, or transmit criminal justice information.
- Guaranteeing the security, integrity, and availability of service needed by the criminal justice community.

2.3 RMS Program Leaders

Each participating agency shall designate to the Program Manager a Program Leader to represent their agency.

2.4 RMS Program Leaders Responsibilities

The RMS Program Leaders (PLs) located at participating agencies shall be responsible for the following:

- Ensure appropriate use, enforce system discipline, and ensure RMS operating procedures are followed by all users of the respective telecommunications links.
- Approve RMS systems access, only after approval from PM
- Assume ultimate responsibility for managing the security of RMS systems within their agency.
- Manage, maintain, and documents agency RMS updates.
- Forwards all updates to the PM.

- Identifies who is using the hardware/software and ensure that no unauthorized users have access to same.
- Identifies and documents how the equipment is connected to the RMS network.
- Ensure that personnel security screening procedures are being followed as stated in this policy.
- Ensure that appropriate hardware security measures are in place.

3 Security Enforcement

3.1 Purpose

Each participating agency shall be responsible for enforcing systems security standards for their agency, in addition to any other entities which may provide technical or contractual support to equipment which interfaces the RMS or county network. Interface agencies shall have documented procedures in place to monitor all security policies outlined herein, including those procedures through state and local programs which meet or exceed these requirements. Participating agencies shall provide written security policies to the PM.

3.2 Standards of Discipline

Authorized users shall access RMS systems and disseminate RMS data only for the purposes for which they are authorized. Each participating agency authorized to access RMS systems shall have a written policy for the discipline of RMS policy violators if an agency or department policy does not already exist. Any infractions of the policy shall be reported to the PM, including corrective or disciplinary actions to the violator. Violations which constitute a violation of law shall be reported to the Sheriff for investigation and enforcement action.

3.3 Awareness and Training

Each agency PL shall ensure that security awareness training is conducted for all users and all appropriate IT Personnel within six (6) months of their appointment or assignment. Documentation of completed security awareness training shall be forwarded to the PM.

4 Physical Security/Site Security

4.1 Purpose

The purpose of the Physical Security Requirements is to ensure that the RMS, County network, and the information stored therein is protected from unauthorized access. Sheriffs Office (SO) will make every effort to avoid undue hardship to other participating agencies, however the standards will be applied to every agency connecting to the RMS and County network.

4.2 Computer Facility Security

The computer site and related infrastructures (e.g., information systems servers, controlled interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc., including law enforcement vehicles if they house equipment which provides access to the RMS/County network) must have adequate physical security at all times to protect against unauthorized access to computer devices, access devices, and printed and stored data.

4.3 Visitor Access

Any person not authorized access to RMS by the PM shall be escorted by authorized personnel at all times when entering computer centers, or terminal areas, or interconnecting facilities.

5 Personnel Security

5.1 Purpose

The purpose of the Personnel Security Enforcement is to ensure that the RMS and the county network and the information stored therein is protected from unauthorized access. Employee backgrounds, the reuse, and disposal of media are key elements to enhance security, for prevention of unauthorized access or dissemination of information.

5.2 Personnel Background Screening for systems access and Computer Terminal/Records Storage Areas Access

- A background check shall include at minimum a national fingerprint database check and NCIC/TCIC criminal history check shall be conducted prior to having authorized access on each person whom RMS access is sought. All requests for

systems access shall be made through the PM. The PM, or their official designee, is authorized to approve RMS systems access.

- The PM shall deny access to any person with a felony conviction, record of any kind indicating a security threat or risk, or on whom information received indicates is under investigation for any felony, or theft, or involvement in organized criminal activity. The PM shall report to the participating agency seeking access reasons for any denial. The Participating Agency may petition the Sheriff for a variance and approval if extenuating circumstances exists.

- If the person is employed by a non criminal justice agency, the PM or his/her official designee shall review the matter to determine if systems access is appropriate.

- The PM may grant access to RMS to a person who has current access NCIC/TCIC prior to completion of a background check when required.

5.3 Disposal of All Media

- When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process RMS data shall be destroyed by cross cut shredding, overwrite applications, incineration, or degaussing, considering whichever method is available, appropriate, and cost effective. This list is not all-inclusive.

- IT systems which have processed or stored RMS data shall not be released from control of the participating agency until the equipment is sanitized and all stored information has been cleared. The sanitation method shall be approved by PM.

5.4 Media Reuse

Electronic storage media that will be reused by another entity shall be sanitized by degaussing or by an overwrite application. The steps taken to sanitize shall be documented by the releasing agency.

6 Network Security Violations

6.1 Network Security

Participating agencies connecting to RMS services shall provide firewall protection, anti-virus protection and spyware protection between their network and the interconnection to

the county/city network infrastructure. The PLs will be the point of contact on security-related issues for their respective organizations. Participating access may be suspended for network security violations.

6.2 Incident Response

PM responsibilities shall include:

- Managing and maintaining the RMS Network Security
- Serving as a central clearinghouse for all reported intrusions, incidents, security alerts bulletins, and other security-related material
- Ensuring additional resources for all incidents affecting RMS systems as needed
- Disseminating prompt advisories of systems threats and operating system vulnerabilities to all agencies through the use of a email distribution list, to include but not limited to:
    - Product Security Bulletins
    - Virus Bulletins,
    - Worm, Malware, Spyware threats

PL responsibilities shall include:

- Coordinate with the PM concerning incident handling and response
- Reporting incidents within their area of responsibility to the PM

6.3 Identifying Network Incidents

The following is a partial list of network incident indicators that would be considered reportable:

- The system unexpectedly crashes without clear reasons
- New user accounts are mysteriously created which bypass standard procedures
- Sudden high activity on an account that has had little or no activity for months
- New files with novel or strange names appear
- Accounting discrepancies
- Changes in file lengths or modification dates
- Attempts to write to system files
- Data modification or deletion
- Denial of service
- Unexplained poor system performance
- Anomalies
- Suspicious probes

- Suspicious browsing

These indicators are not proof that an incident has or is occurring. However, it is important to suspect that an incident might be occurring and act accordingly.

6.4 Investigating Incidents

Responsibilities for computer incident response shall include:

- Notify the PM or designee either by telephone or e-mail within four hours after the resolution of security incident on a network. However, if an RMS workstation or network device may be compromised, the point of contact shall immediately notify the PM by calling the Sheriffs Office.
- Document the incident from beginning to end
- Determine the nature and scope of the incident:
    - Look for modifications to system software and configuration files
    - Look for tools installed by the intruder
    - Check other local component systems for modifications
    - Notify the PM
- Resolve the problem and get the system back to normal operations. If an intrusion is in progress, make a risk-based management decision to either leave the system attached or disconnect from the network. **DO NOT POWER DOWN THE SYTEM.** This may cause the loss of valuable information regarding the intrusion. Preserve the evidence by performing the following:
    - Copy log files
    - Review log files
    - Check binaries and configuration files

Any system which has been compromised shall not be used until it has been "cleaned."

6.5 Reporting

The PLs shall be responsible for collection incident information and providing written reports to PM. In addition, the PM is responsible for notifying the PLs on intrusion information that may affect Interface Agency Systems. Notifications of intrusions/incidents shall be secured in a manner commensurate with the sensitivity of the information being transmitted. Wherever possible, all transmission regarding incidents and/or intrusions will be handled in a secure manner.

Policy violations shall be reported to the PM. The agency shall immediately remove any employee from assignments covered by this policy for security violations pending investigation. Any violation of system discipline or operational policies related to system discipline are grounds for termination, which shall be immediately reported to the PM in writing.

Must report violations of law or suspected violations of law to the Sheriff, along with indications of actions taken by your agency. Failure to report violations can justify termination of the agreement.

Upon notification, the Sheriff's Office reserves the right to:

- Investigate or decline to investigate any report of unauthorized use;
- Suspend or terminate access and services, including the actual telecommunications link. The Sheriff will provide the agency with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the Sheriff.

The Sheriff reserves the right to audit the agency's operations and procedures at scheduled or unscheduled times involving the RMS system. The Sheriff's Office is authorized to perform a final audit of the agency's systems after termination of the RMS utilization.

- Misuse of the RMS system and information under this policy includes:
    A. obtains information in an unauthorized manner, uses the information for an unauthorized purpose or discloses the information to a person who is not entitled to the information;
    B. provides any unauthorized person information obtained either directly or indirectly from the RMS system for any reason.

- Any unauthorized disclosure may result in departmental disciplinary actions to include termination and/or prosecution for violation of applicable criminal laws including:
    A. Texas Penal Code, Section 37.10, Tampering with Government Record
    B. Texas Penal Code, Section 39.02, Abuse of Official CapacityTexas Penal Code, Section 39.06, Misuse of Official Information

- Misuse of the criminal history information in RMS or through TLETS/NLETS access may result in additional criminal penalties by breach of Texas Government Code; Section 411.085, Unauthorized Obtaining, Use, or Disclosure of Criminal History Record Information.

7 Technical Security

7.1 Documentation of Network Configuration

The PM shall document, maintain, and update criminal justice information network configurations and shall distribute these procedures and any changes to the Interface Agency's direct users. The PLs shall ensure that a complete topological drawing which depicts the interconnectivity of the Interface Agency's network configuration is

maintained in a current status by the Interface Agency. This topological drawing shall include the following:

- All communications paths, circuits, and other components used for the interconnection, beginning with the organization-owned system(s) and traversing through all interconnected systems to the organization end-point.
- The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown. An annotation of the number of clients and their ORI designations is sufficient.

- Records of wireless device ID numbers and contact numbers of commercial wireless providers shall also be maintained to allow for deactivation of lost or stolen devices.

7.2 ***Physically Secure Location***

7.2.1 Introduction

The definition of a "physically secure location" is provided to ensure a universal understanding of what this phrase means within the context of the *RMS Security Policy*. It is important because it forms the basis for the proper implementation of Advanced Authentication which follows.

7.2.2 Definition

A "physically secure location" is a criminal justice facility, an area, a room, a group of rooms, or a police/sheriffs vehicle that is/are subject to criminal justice agency management control/security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch 18 panels, etc.) that provide access to the RMS network. Physical security perimeters shall be defined by the PM. Law enforcement sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access. Every physical access point to sensitive facilities or restricted areas housing information systems that access, process, or display RMS data shall be controlled/secured in a manner which is acceptable to the PM during both working and non-working hours.

7.3 Advanced Authentication

7.3.1 Definitions and Policies for Advanced Authentication

There are several means of authenticating a user's identity which can be used alone or in combination with other identity factors:

Definition:

- **Virtual Private Networks (VPNs)** use security mechanisms to effectively create a private network across a shared (usually public) communications backbone connecting distributed elements or members of a single organization. The interconnecting communications backbone may consists of leased lines, dial-up service, packet and cell switched connection oriented networks, and/or routed connectionless networks. VPNs are also useful in restricting distribution among subsets of the organization at large.

Typically VPN's may be utilized to securely communicate between:

- Site-to-site infrastructure across a public communications backbone.
- Local Area Network (LAN)-to-LAN subnets operating across a network that services other entities outside the VPN community.
- Host-to-host workstations across a shared network or subnet.

Policy for VPNs:

- The system shall implement VPN mechanisms using technologies such as cryptography, key management, access control, authentication, and data integrity. The system shall conform to Internet Engineering Task Force (IETF) Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) protocol as specified in RFC 2406. The system shall utilize cryptographic modules that are compliant with Federal Information Processing System (FIPS) 19 Publication 140-2 for "Security Requirements for Cryptographic Modules." The system shall also perform key management and key exchange using the IETF specified Internet Key Exchange (IKE) (RFC 2409) which shall be FIPS Publication 140-2 compliant. i At a minimum, a user shall be restricted from establishing a VPN session without first being identified/authenticated by no less than a userid and password. Identification/authentication can take place at the network, device, application, and/or device/software levels.

- At a minimum, a user shall be restricted from establishing a VPN session without first being identified/authenticated by no less than a userid and password. Identification/authentication can take place at the network, device, application, and/or device/software levels.

7.3.2 Non-secure Locations

Any procurement or upgrade for systems which is considered part of, or is accessing a RMS (Record Management System) from any Internet, wireless, or dial-in connection from a location that is **not** physically secured shall use advanced authentication as defined in this policy.

All mobile devices such as Personal Digital Assistants (PDA), cellular phones transmitting RMS data, and mobile data computers or other portable clients which have been removed from a police/sheriffs vehicle, at a minimum shall also incorporate the use of a unique password or other personal identifier (PIN) as well as meet the advanced authentication requirement.

7.3.3 Secure Locations

Any procurement or upgrade for a system which is considered part of, or is accessing a criminal justice information system between secure locations via the Internet, wireless, or dial-in connection from a remote location, shall use, at a minimum, a Virtual Private Network (VPN) or any combination of security tools that provide approved encryption and advanced authentication as defined in this policy.

7.4 System Logon

7.4.1 Identification/Userid

Each person who is authorized to store, process, and/or transmit information on an RMS system shall be uniquely identified by use of a unique identifier. A unique identification shall also be required for all persons who administer and maintain the system(s) that access RMS data. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Organizations shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Organizations shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users.

7.4.2 Authentication/Password

7.4.2.1 Introduction

Authentication refers to mechanisms or processes which verify that a user really is who they say they are once the person is uniquely identified. Authentication of each user's identity can be a userid and unique password combination implemented at a local agency.

7.4.2.2 General Authentication

Each individual's identifier/password shall be authenticated at either the local Interface Agency and the RMS level.

7.4.2.3 Passwords

If passwords are used for authentication, organizations shall ensure the following secure password attributes:

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

7.5 Access Control

The Interface Agency shall develop and maintain the security documentation to address access control.

7.5.1 Screen Saver

Computer systems shall be equipped with a screen saver. Computer will be set with a 10 minute idle time criteria. Screen saver will be configured with a password login.

7.6 Internet Access

The PM is authorized to grant Internet access to support RMS processing when a minimum set of technical and administrative requirements have been met, to include advanced authentication and encryption. To assure the security of RMS systems from unauthorized Internet access and to preserve the confidentiality, integrity, and availability of RMS information as it is processed, RMS transactions shall be permitted over the Internet only after the following minimum requirements have been implemented:

- Advanced authentication as defined within this policy.
- Networks in which some terminals or access devices have RMS access and/or Internet access (e.g., peer-to-peer relationships, large mainframes and servers that house web sites) shall be protected by firewall-type devices. These devices shall implement a minimum firewall profile in order to provide a point of defense and a controlled and audited access to servers, both from inside and outside the RMS networks.
- Data which is at risk on access devices and workstations shall have the residual RMS data protected by the methods of removal, encryption, or erasure.
- All CJIS data transmitted through any Internet connection shall be immediately protected with a minimum of 128 bit encryption.
- All Internet connections shall support a minimum of 128 bit encryption

7.7 Encryption

- All RMS data transmitted through any public network segment or over dial-up or Internet connections (does not include radio frequency transmissions) shall be immediately protected with a minimum of 128 bit encryption. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct management control of a criminal justice agency.
- All connections requiring encryption shall have a minimum of 128-bit encryption.
- Encryption may terminate either at a router or firewall within a secured location, or the data may be encrypted from client to client. While client to client encryption is encouraged, it is not a requirement as long as the RMS data passing as clear text is doing so within a secured facility behind a properly configured firewall.

7.8 Wireless

- All wireless connections shall support a minimum of 128-bit encryption for all data.
- All currently-in-use symmetric and asymmetric mobile data terminal crypto-systems shall have key lengths of at least 56 bits or more; however, these

currently-in-use systems shall meet the minimum 128-bit encryption requirement for data.

For your information:

- *Asymmetric encryption is the same as public-key cryptography, i.e., a form of cryptography in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key, and the receiver decrypts them using the private key. Using this method, the private key never has to be revealed to anyone other than the user.*
- *In symmetric cryptography, both ends have the same encryption key, meaning it uses the same key for encryption and decryption.*

- All wireless links or server access points must be protected by authentication to ensure protection from unauthorized system access.

7.9 Firewalls

NOTE: While physically secured locations that house equipment which allow access to the RMS network must meet the following firewall requirements, police/sheriffs vehicles are not subject to these firewall requirements.

- Networks in which some terminals, and/or access devices have RMS access and/or Internet access (e.g., peer-to-peer relationships, large mainframes and servers that house web sites) shall be protected by firewall type devices. These devices shall implement a minimum firewall profile in order to provide a point of defense and a controlled and audited access to servers, both from inside and outside the RMS networks.
- Firewall architectures shall prevent unauthorized access to RMS data and all network components providing access to the RMS WAN, either directly or indirectly through connections to other networks. Firewall policies shall be concerned with securing the total site. This must include all forms of access, wireless, dial-in, off-site, Internet access, and others.
- Firewall operating system builds shall be based upon minimal feature sets. (It is extremely important that all unnecessary operating system features are removed from the build prior to firewall implementation, especially compilers.) All unused networking protocols shall be removed from the firewall operating system build.
- Any appropriate operating system patches shall be applied before any installation of firewall components, and procedures shall be developed to ensure that the firewall patches remain current while the firewall retains its statefullness.
- All unused network services or applications shall be removed or disabled. Only network services that are required shall be permitted through the firewall. Allowed services shall be documented as to the service allowed, the description of service, and the business requirement for service.
- All unused user or system accounts shall be disabled

- All default vendor accounts shall have the passwords changed prior to the firewall going on-line
- Unused physical network interfaces shall be disabled or removed from the server chassis.
- Only firewalls employing multiple network interfaces (a.k.a. dual-homed) are permitted. A firewall having less than two network interfaces or otherwise conducting inbound and outbound traffic on a single network line shall not be permitted.
- A firewall implementation shall not reside on a shared server platform offering general network file and print services to a user community.
- All firewalls shall be backed up immediately prior to production release. (As a general principle, all firewall backups should be full backups as there is no real requirement or need for incremental backups.)

7.10 Firewalls

All IT systems with RMS connectivity shall employ virus protection software. Anti-virus software shall:

- detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways
- be enabled on workstations and servers at start-up and employ resident scanning; and
- on servers, update virus signature files immediately, or as soon as possible, with each new release.