**RESPONSE TO GRAND JURY REPORT FORM**

**Report Title: MENDOCINO COUNTY'S TRAILING INFORMATION TECHNOLOGY**

**Report Date: July 16, 2021**

**Response by: Mendocino County Sheriff' Office**

**FINDINGS**

- I (we) agree with the findings numbered: F4
- I (we) disagree wholly or partially with the findings numbered: F5 and F6.

  (Attach a statement specifying any portions of the findings that are disputed; include an explanation of the reasons therefor.)

**RECOMMENDATIONS**

- Recommendations numbered R4 will not be implemented because they are not warranted or are not reasonable.

  (Attach an explanation.)

Date: January 11, 2022 Signed:_____

MATTHEW KENDALL, Sheriff
Mendocino County

Total number of pages: 16

## RESPONSE SUMMARY

Since the 2015-2016 Grand Jury Report, no discernable policy or procedure has been created or implemented by the Mendocino County Board of Supervisors ("BOS") to solve the problems between the SHERIFF IT and COUNTY IS. The COUNTY IS still retains control over the Sheriff's email system and is thereby able to grant any user "Administrator" access to the Sheriff's email system to anyone. If consolidated, the "Administrator" would then have access to the Sheriff's entire computer and email system. History has shown that when such access was granted by the COUNTY IS Director to an Assistant CEO the power was abused.

State law outlines the operational procedure required for a connection to the Department of Justice Computer system. These statutes clearly indicate the Sheriff by law shall have **sole and exclusive authority** over his network, data, and computers.

These secure connections to DOJ and NCIC computer systems allow us the ability to effectively detect and investigate crimes. They are also necessary in many mandated entries into the system including: missing persons; stolen and recovered property; tracking of firearms; wanted persons; functions of housing and maintaining our inmate populations; and reports to the California Department of Justice. These statutes mandate that the Sheriff must maintain sole and exclusive authority over his entire IT infrastructure, including: the email system; hiring and managing his IT staff; and, maintaining a strict chain of command necessary for the investigation and detection of crime. In addition, the Sheriff must maintain the ability to hire/terminate staff within Department of Justice ("DOJ") requirements/regulations to guarantee compliance and the integrity of his infrastructure. There can be no dotted or blurred lines in the areas of responsibility or accountability when it comes to access to highly sensitive data.

Having an IT system that includes total control over email either generated by or sent to the Sheriff's Office completely independent of COUNTY IS, is just one major part in protecting confidential information, witnesses, informants, and you.

## REQUIRED RESPONSE TO FINDINGS

**F4. The Sheriff agrees.**

The BOS chose to fund only a small portion of the Intellectual Technology Master Plan ("ITMP") for the County and Sheriff. There are a majority of initiatives left behind and unfunded by the BOS. There are also mandatory operating costs and upgrades that the CEO/BOS refused to allow to be included in the Sheriff's budget. This puts public safety, officer safety, and Federal/State compliance at risk.

**F5. The Sheriff disagrees.**

The Grand Jury Report does not accurately represent the actual Federal/State law or what was presented to the Grand Jury. The Sheriff currently operates his computer network under a "hybrid" model with the County. The Sheriff leverages as much assistance and support from COUNTY IS that is allowed under Federal and State Law. However, there is a point at which the Sheriff must maintain control over physical and virtual security to comply with the law and not compromise his investigations.

**F6. The Sheriff disagrees.**

Said finding is ambiguous since it is not possible to discern whether the clearance referred to is from the Sheriff or some other department head. Currently the Sheriff maintains sole and exclusive authority over the current SHERIFF IT infrastructure, including hiring and managing his staff, but does not have the same control over the email system. Under the current system only one employee at COUNTY IS has received approval to work on networking equipment related to the Sheriff's network. The remaining COUNTY IS staff have NOT received such approval.

## REQUIRED RESPONSE TO RECOMMENDATIONS

**R4. The Sheriff disagrees.**

**1. Agency Head and Control Host.** In spite of public representations made by the County Counsel, neither the CEO, Board of Supervisors, County Counsel or his office, have control over Federal and State DOJ connections or the right to access data from the DOJ directly. County Counsel is not the System Control Host or the Agency Head of the Sheriff's Office. Claims that "we are good with the DOJ" are beyond the County Counsels ability to report accurately on. Only the Sheriff (Agency Head/Control Host) can accurately report on the status of the DOJ agreement and relationship after intensive annual audits by the State/Federal DOJs for compliance with the agreement.

The Sheriff is the Agency Head and Control Host to the Federal and State DOJ. DOJ data is disseminated to County Counsel only on a "right to know" ***and*** "need to know" basis. This data is provided to the Sheriff, DA, and other state and local law enforcement agencies. The County Counsel has no permissions to directly access or control the DOJ connection. Only the Sheriff is responsible for compliance of downstream DOJ agencies within the County in addition to Probation, HHSA SIU, and the Superior Court. Audits of these agencies and their compliance is within the Sheriff's area of responsibility.

**2. Failures to comply with Federal/State DOJ regulations.** The Sheriff has no direct or indirect control over COUNTY IS. As a result, COUNTY IS employees are not required to pass as a condition of employment a full background check that complies with the Federal/State DOJ regulations. Failure to comply with those regulations can result in the Sheriff being locked out of their systems, which could have a substantial negative impact on the Sheriff's Office being able to perform its duties as set forth in the California Constitution and state law.

There are numerous examples of COUNTY IS employees that: made active threats against the SHERIFF'S IT network, which threatened the integrity of the entire computer and email system; maintain PC's and other equipment in all locations including the DA, Probation,

and Public Defender that was on active felony probation; and, could not have passed the background check required by Federal/State DOJ regulations.

The following are three (3) examples include two (2) of the most egregious violations of security protocols. The third relates to a filter installed in the email system which blocked the Sheriff from communicating with his attorney regarding a matter related to pending litigation.

As to the first two examples, according to two former Directors of the COUNTY IS:

1. In about 1992, the COUNTY IS Director was recruiting to hire for a newly created COUNTY IS Security Officer. He wanted to hire a personal friend but was informed that the fried had failed the Sheriff's Office background investigation. The Undersheriff voiced his concerns about filing the position with a person who had a felony conviction but was ignored. The individual was hired by COUNTY IS in spite of the Undersheriff concerns. As the COUNTY IS Security Officer, he had unfettered access to the information system and data of the Mendocino County; Superior Court; District Attorney; Probation Department; and, all other Mendocino County departments. The Sheriff's Office was the only department that was able to block his access. The COUNTY IS Security Officer resigned his position in 1996 after the COUNTY IS Director was terminated and COUNTY IS was absorbed into the General Services Department in April 1996.

2. In about 2015, a former Assistant CEO who had direct supervisory authority over COUNTY IS, gained access to the entire county computer network and email system by demanding a former COUNTY IS Director make him an "Administrator". The former COUNTY IS Director yielded to the demands when he felt his department was being threatened financially, if he did not comply, with: a substantial reduction in his: office space; office staff; and, funding for the Sheriff's Public Safety Microwave System. Becoming an "Administrator", allowed the former Assistant CEO to access to the entire computer network system including the email auditor function and ability to surveil confidential internal documents and communications of between various County employees and departments.

Multiple times over the course of the next few months the former COUNTY IS Director sought to cancel access by the former Assistant CEO. Each time the former Assistant CEO thwarted his efforts by explaining he was not done looking around and wanted to maintain access. Out of fear of retribution, the former COUNTY IS Director did not cancel his access capability. The breach was not immediately reported to County departments and the abuse continued for several months without department heads being aware the Assistant CEO had full access to their communications, confidential or otherwise.

Although the offending Assistant CEO is no longer employed by the County, it remains a prime example of how easily an individual in power can abuse his authority. Safeguards are useless when the COUNTY IS Director is ordered to by the Assistant CEO or his superior, under threats of retaliation, to grant him unfettered access to the computer and email system.

The 2015-2016 Grand Jury, in their report titled "Mendocino County Policy 22 - Who Has Access", reported on the potential abuse of the email systems "highly sensitive and confidential messages within the Offices of the County Counsel, the District Attorney, Human Resources, the Sheriff, and the Board of Supervisors and Grand Jury". To quote that report:

> "Because of the inability of the County email software to segregate super-user access to specific accounts, access by management to employee email is unrestricted. Super-user email access is all or nothing. While in place, any County manager who is granted access, has complete and total access to all email accounts in the County system. This leaves the County exposed to legal risks and potentially creates the opportunity for a 'dirty admin' to abuse the email system. As a super-user with access to the mail auditor function, any County manager may obtain unrestricted access to highly sensitive and confidential messages within the Offices of the County Counsel, the District Attorney, Human Resources, the Sheriff, and the Board of Supervisors and Grand Jury, to name some examples. The Grand Jury received allegations that this system of unrestricted access has led to abuses."

The term "super-user" is defined in Policy #22 as follows:

> "Super-user - A departmental staff person whose normal job does not require IT-related activities, but, for whatever reason(s), has a greater than average understanding of a particular application. Due to this enhanced skill set, this person may assist other users with a particular program(s)."

The use of the term "super-user" by the 2015-2016 Grand Jury implies that additional persons below the management level of Assistant CEO may have also been granted "Administrator" access which would mean a much greater breach of the computer system than has been reported.

The third example is an interference with the email system controlled by COUNTY IT. On November 10, 2021, at 2:24 PM, an email was sent by the County Counsel to the email address of the Sheriff's attorney of record in the Mendocino County Superior Court case captioned MENDOCINO COUNTY SHERIFF MATTHEW KENDALL V. MENDOCINO COUNTY BOARD OF SUPERVISORS, case number 21CV00561. The letter was regarding a Mendocino County Board of Supervisors special meeting scheduled for the next Monday, November 15, 2021, where the Board would enter into a contract with an attorney to represent the Sheriff in various matters where the County Counsel had a conflict of interest. That issue of who was going to represent the Sheriff in the various matters where the County Counsel had a conflict of interest was already under submission with the court and awaiting a decision after multiple court hearings. According to email it was sent to the Sheriff's attorney of record in the above-entitled action lawsuit against the Board of Supervisors at lawoffice@duncanjames.com. That was the office email address for said law office since the account was first established more than twenty (20) years ago. The letter was cc'd to the Sheriff.

At approximately 8:15pm on the evening of November 10, 2021, the Sheriff called his attorney regarding the email and was told it was never received from the County Counsel. The Sheriff was asked to forward the email which the Sheriff unsuccessfully attempted to do.

The next morning the Sheriff and his attorney had multiple phone conversations regarding the content of the email since it needed some form of immediate response. The

Sheriff's attorney again asked for the email to be forwarded, which the sheriff again unsuccessfully tried on three (3) separate occasions. The Sheriff's attorney then asked the Sheriff to send the email to the SHERIFF IT Director to see if he could successfully forward it. The SHERIFF IT Director successfully received the email at issue from the Sheriff but when he tried forwarding it to the email addresses for the Sheriff's attorney it was blocked. The SHERIFF IT Director received an automatically generated notice that the email was blocked. The SHERIFF IT Director said it is very clear that the block on those addresses is on the County GroupWise email server as the email does not appear to leave the County server and is blocked and returned immediately to the sender.

This is just another example of why the two IT systems cannot be merged and emphasizes why the Sheriff needs a totally independent IT and email system over which the COUNTY IS has no administrative or other control.

Trusting the confidentiality of the email system to Administrators that do not report directly to the Sheriff is recipe for failure and abuse. The County itself has no comprehensive background investigation. They may fingerprint employees but a full pre-employment background investigation such as conducted by the Sheriff does not occur. In fact, the County has demonstrated that they are willing to hire people on active felony probation or with criminal history's that is not congruent with the integrity of the Sheriff's Office.

**3. <u>Future Potential Abuses.</u>** Since the 2015-2016 Grand Jury Report, neither the CEO or Board of Supervisors has done anything substantive to protect against future abuses. COUNTY IS still retains control over the Sheriff's email system and is thereby able to designate any person it chooses as an "Administrator", which would grant them access the Sheriff's email system; or, install any filters they wished to control the email received by the Sheriff. There is no evidence history will not repeat itself.

Changing the title of a county management employee in the CEO'S office to whom the COUNTY IS Director reports does nothing to change or resolve any of the issues. There can be

no dotted line between the Sheriff and his data. Dotted or blurred lines of reporting, lead to confusion in areas of responsibility and potential abuse. Abuse has occurred and there is no way to overcome that kind of abuse without giving the Sheriff a comfort level of being in exclusive control of his computer network and email system.

All aspects of the Sheriff's computer system are critical tools in his fight against criminal activity in the county. On a daily basis, the Sheriff has many issues to address including: criminal investigation; suspects; witnesses; and, informants. This email system is not a system where employees are emailing friends and family. It is a system where the Sheriff is in constant communication with: witnesses to crime; citizen informants; confidential informants; other state, county and city law enforcement agencies and their investigative staff; state and federal law enforcement agencies, including but not limited to the United States Attorney General, FBI and Homeland Security Offices throughout the country; branches of the United States military; and, state and federal crime labs, to name just a few; and, last but not least, his attorney. Witnesses and confidential informants' perception of the Sheriff being trustworthy and willing to protect their confidentiality is essential to successful investigation. If victims, witnesses and confidential informants lose faith in the Sheriff's ability to protect their identity, the Sheriff may lose their willingness to cooperate. If they then do not cooperate, crimes will not be solved.

When the Sheriff does not have control over his own computer network and email system, he cannot assure that witnesses or confidential informant names, address and phone numbers will remain confidential since he would have no control over the administration of the system or supervision authority over the employees with access thereto.

Even within the Sheriff's Office there are built in fire-walls that limit access to information to those persons who are in a right-to-know and a need-to-know status. For example, a Corrections Officer has no need-to-know the contents of criminal investigation reports and intra or inter-office (email) communications and is thereby blocked from accessing that information. A Bailiff has no need to know the names, addresses and cell phone numbers of

the percipient witnesses and confidential informants that may be witnesses to the offense and is thereby blocked from accessing that information. These layers of accessibility are in place in order to preserve the integrity of information therefore allowing detection and investigations of crime.

A full pre-employment background investigation by the Sheriff does not just involve fingerprinting. Each potential employee is subjected to an intense full background investigation, many of these include psychological evaluations, polygraph examinations and full personal history statements. Often family members, neighbors, co-workers are interviewed during these investigations.

These background investigations are often invasive and generally give the Sheriff a confidence level in the staff he is hiring to protect the integrity of the Sheriff's Office. Many potential employees do not pass these background checks and are not hired. The public should be aware that the Sheriff will not compromise when it comes to best practices for hiring, vetting, and maintaining integrity of his staff. Having a confidential IT system completely independent of COUNTY IS computer network and email system is just one major part of the Sheriff's tool chest needed to protect witnesses, confidential information and informants, and you.

**5. <u>Mendocino County Policy #22</u>**. Policy #22 is titled "Information Technology (It) Policy: Acquisition, Software, the Role of the Information Technology Committee, The Role of Information Services and the Role ff Departmental IT Personnel." It is a major impediment to the Sheriff's ability to operate the SHERIFF IT computer network. It is also used by the CEO to control maintenance, repair and replacement of the SHERIFF IT, in violation of federal/state laws and regulations. The policy as adopted in 2003 is antiquated and impacts all aspects of:

1. The selection and acquisition of hardware (PC's, Servers, Network, other devices);
2. The selection and acquisition of software (cloud based, self-hosted, etc); and,
3. The hiring/managing of staff.

Therefore, the Sheriff objects to those provisions of Policy #22, in part, as follows:

| SECTION | OBJECTION |
|---|---|
| **"SECTION I- ACQUISITION"** | |
| "2. Major System Procurement: Major proposed procurement of application software and/or computer hardware for new systems or major enhancements to existing systems must be submitted to Information Services and to the Information Technology Committee for review and recommendation." | 1. The Sheriff objects to this policy on the following basis; "The person designated as a county's 'control agent' […] shall have sole and exclusive authority to ensure that the county's or other agency's equipment connecting to the California Law Enforcement Telecommunications System ["CLETS"] complies with all security requirements that are conditions of access to the [CLETS] under the provisions of this chapter, or the policies, practices, and procedures adopted pursuant to Section 15160, and that the equipment complies with the county control agent's security policy. This authority shall include, but not be limited to, locating, managing, maintaining, and providing security for all of the county's or other agency's equipment that connects to, and exchanges data, video, or voice information with, the [CLETS] under the provisions of this chapter, including, but not limited to, telecommunications transmission circuits, networking devices, computers, data bases, and servers." (California *Government Code* §15164.1(a.).) |
| "3. Minor System Procurement: Minor computer hardware and software additions or enhancements to existing application systems must also be reviewed by Information Services to ensure continuing compliance with County guidelines." | 2. See Objection #1 above. |
| "4. Fixed Asset Procurement Procedure and Inventory: General Services is responsible for the purchasing of computer hardware and software through the standard requisition/purchase order process. General Services will not process a requisition/purchase order unless it is supported by documented approval from Information Services." | 3. See Objection #1 above. |
| **"SECTION II - OWNERSHIP AND USER OF COMPUTER HARDWARE AND** | |

| SECTION | OBJECTION |
| --- | --- |
| **SOFTWARE"** | |
| "1. Computer hardware and application software systems purchased with County general funds are the property of the County, not of individual departments, and may be subject to reallocation as the needs of the County change." | 4. This puts DOJ data at risk and will not be allowed by the Sheriff as written, especially not at the discretion of the CEO. The decision on "needs of the County" as it relates to criminal activity is not a matter subject to control by the CEO/BOS. These whims could be used to control or manipulate the Sheriff's ability to detect and prevent crime, operate the jail, and meet all other constitutional mandates.<br><br>PC's, servers, databases, network equipment, etc., generally all contain DOJ protected data. None of these devices will be reallocated at the discretion of the CEO/BOS. Strict rules apply to the storage of data, repurposing, and recycling of devices which are enforced by the Sheriff. Failure to comply with the laws and regulations can result in the Sheriff's access go the system being blocked |
| "2. All County computers and networked equipment property ownership rights are vested in the County of Mendocino and are subject to the controls, policies, and procedures established by the Board of Supervisors and the County Administrative Office." | 5. See Objection #1. The entire network, but not limited to the entire network is under the sole and exclusive authority of the Sheriff, not the BOS/CEO/CAO/CIO. |
| "5 [2nd para., 1st sentence]. The County owns or has unlimited right to access any and all information and data stored on County-owned, -leased, or -controlled computers, equipment, or networks. County management reserves the right to access any information or data, including electronic mail, stored on County-owned, -leased, or -controlled computers." | 6. This is a gross violation of the Sheriff's right to conduct private investigations and protect his DOJ derived data.<br><br>See: California Government Code (GC) § 15150 through § 15167; and, the entire FBI/DOJ Criminal Justice Information Services (CJIS) Security Policy |
| "5 [2nd para., 2nd sentence]. Any passwords shall be provided to the appropriate department head upon request." | 7. See Objection #1 above. This is a violation of the DOJ agreement.<br><br>Sharing of passwords is categorized as a "system misuse" and is prohibited. The County does not |

| SECTION | OBJECTION |
| --- | --- |
| | follow best practices, but the Sheriff does and he is mandated to uphold the State and Federal law.<br><br>(See California Government Code (GC) § 15150 through § 15167; and, California Law Enforcement Telecommunications System Policies Practices and Procedures ("CLETS-PPP") §1.10.1 of the CLETS-PPP. |
| "10. Information Services is authorized to conduct audits of County-owned, - leased, or -controlled computers and networked equipment to ensure that County policies and procedures are being followed." | 8. See Objection #1 above. There are many violations of the DOJ regulations.<br><br>This is system misuse. The "right to know" and "need to know" are not congruent with this local county policy. The Sheriff must retain strict control over his network, PC's, servers, databases, etc. Any investigations can only be done at the discretion of the Sheriff.<br><br>This is neither acceptable to the Sheriff nor consistent with Federal/State law. No audit of the SHERIFFS IT can occur except by persons who are specifically approved for such audits by Federal and State Departments of Justice and approved by the Sheriff.<br><br>(See California Government Code (GC) § 15150 through § 15167; and, CLETS-PPP") §1.10.1 of the CLETS-PPP.) |
| **SECTION IV - THE ROLE OF INFORMATION SERVICES** | |
| "1. Information Services is charged with the delivery of IT services to all County departments. To the greatest extent possible, Information Services shall appoint and manage IT support staff." | 9. This is not acceptable to the Sheriff. He must maintain hiring/firing discretion of his staff to keep his investigations confidential and his DOJ derived data secure.<br><br>CLETS PPP 1.9.2: Required background checks for unescorted staff, and the agency head will be the hiring determination.<br><br>CFBI/DOJ CJIS 5.12: Personnel Security strict guidelines for hiring and maintaining compliance in meeting background check. |
| "3. Information Services may, at its | 10. See above Objection 9, also the Sheriff |

| SECTION | OBJECTION |
|---|---|
| discretion, conduct assessments of the technical services and the IT skill levels of supporting staff. The result of an assessment may cause Information Services to modify the delivery model of IT services in the County, including the assignment of departmental IT personnel. ” | maintains hiring/firing authority<br><br>This is not acceptable to the Sheriff nor consistent with Federal/State law. No assessments of the SHERIFFS IT can occur except by persons who are specifically approved to conduct such assessments by Federal and State Departments of Justice and approved by the Sheriff. |
| **SECTION V - THE ROLE OF DEPARTMENTAL IT PERSONNEL** | |
| “1. No departmental IT positions/staff request shall be presented to the Board of Supervisors without the approval of the Director of Information Services or his/her designee.” | 11. This is not acceptable to the Sheriff or consistent with Federal/State law. Only persons who comply with Federal and Stated standards that have successfully completed a background check conducted by the Sheriff shall be, be presented by the Sheriff to the Board of Supervisors for approval, without comment or inference from Informational Services, or Director of Information Services or designee.<br><br>The Sheriff SHALL have sole and exclusive authority over all security requirements in the CLETS agreement. Including hiring and selection of personnel. This authority SHALL include, but not be limited to… (California *Government Code* §15164.1.) |
| “2. The Director of Information Services, or his/her designee, shall have the authority to comment upon and advise in the hiring of departmental IT personnel and to participate in on-going evaluations of departmental IT personnel.” | 12. This is not acceptable to the Sheriff or consistent with Federal/State law. Only persons who comply with Federal and Stated standards that have successfully completed a background check conducted by the Sheriff shall be, be presented by the Sheriff to the Board of Supervisors for approval, without comment or inference from Informational Services, or Director of Information Services or designee.<br><br>See Objection 11. The Sheriff will include County IS in on-going evaluations of departmental IT personnel at his own discretion. |

## CONCLUSION.

The Sheriff is charged with protecting not only his data but also access to the Federal/State Department of Justice systems. Merging the COUNTY IS system with the SHERIFF IT system, including maintaining a joint email system would expose the system to unauthorized access and cannot occur without the Sheriff's consent.

The COUNTY IS has been historically slow to respond to urgent issues. An example is when the Sheriff's Willits patrol office went down on a Friday afternoon. The issues were determined to be under the COUNTY IS department maintenance of the Microwave system. COUNTY IS staff did not want to work on the issue at night or over the weekend. They are a M-F, 8:00AM to 5:00PM operation. That is not acceptable to the Sheriff and can jeopardize the safety of the deputies, residents and visitors in Mendocino County. The Sheriff's Office does not suspend operations when the weekend or 5:00PM arrives. The entire Sheriff's Office runs and operates on a 24/7/365 basis which includes the Jail, Patrol, Dispatch, 911, and Emergency Services divisions. Each of these divisions is dependent on the operation of the computer system.

In addition, the Sheriff has many investigative needs that are dependent on an operating computer and email system. These needs include verifying or locating specific information relating to such crimes as: murder; child abuse; human trafficking: and, sex offenses in all forms, to reference only a few. And, the names, addresses and phone numbers of the percipient witnesses and confidential informants.

Until you have been involved in the investigation of one of those offenses you cannot comprehend the terror and fear witnesses or confidential informants have of retaliation for the simple reason, they cooperated with law enforcement. Many times, it is a realistic fear for their own safety or life; or, fear for the safety or life of their family, especially when they are cooperative with law enforcement. Whether they are victims, witnesses or confidential informants, they are real people with real emotions. They could be an acquaintance or your neighbor, even though the crime may not have occurred in your neighborhood. Victims,

witnesses and confidential informants need to feel safe and free of fear of possible retaliation against themselves or their family by the suspect or the suspects friends or family, as a result of the inadvertent or intentional disclosure of their name, address or cell phone.

It is difficult enough to be a witness to crime much less the confidential informant who provided the information that resulted in a successful arrest. It is not a movie or tv program you can walk away from at your own choosing. This is real life; real people. Often, victims, witnesses and confidential informants continued cooperation may solely be dependent on their belief the Sheriff will protect their identity. Their ability to feel safe is critical to the Sheriff's ability to bring the accused to justice.

The entire Information Technology system is an integral part of the Sherriff's communication system with the Deputies in the field during quiet times as well as during emergencies. With the Sheriff in control of the SHERIFF IT staff, response times are extremely fast whether the Sheriff's Office is responding to a violent crime, forest fire or flood, a timely response can mean the difference between life and death. The response time must also be fast when there is a glitch or breakdown in the SHERIFF IT computer network. The Sheriff needs the same capability to respond and repair in an emergency fashion where there is a failure in the email and communication systems. Since he does not have control over the email and communication systems, he has to rely on COUNTY IS to respond. As has been previously described herein, COUNTY IS has historically been slow to respond.