Risk Evaluation of the Protection of Private Personal Information Collected by the Doña Ana County Clerk's Office

Conducted by the External Review Committee of the Doña Ana County Clerk's Office

Submitted on September 22, 2015

Summary

On June 1, 2015 Lynn J. Ellins, the Doña Ana County Clerk, was informed of accusations that an employee had used her access in the County Clerk's Office to steal personal private information. The accusation is that she would come in early to work and spend about five minutes writing down the names, Social Security numbers and dates of birth of registered voters. She is accused of providing this information to individuals who used it to file fraudulent tax returns.

On June 9, 2015 Mr. Ellins announced the creation of an External Review Committee (ERC). This committee was tasked to review the security of private information gathered in the County Clerk's Office, compare it to the best practices in the public and private fields, and make recommendations to substantially reduce the risk of a security breech involving this information to the lowest possible level.

Members of ERC include: Russell Allen (chair), Paul Deason, Gwendolyn Hanson, John Hummer and John Muñoz. See Appendix A for biographical information.

The committee met four times to review practices at the county, review research on best practices, talk to county staff and make recommendations for improvements. Other participants included County Clerk Lynn J. Ellins, Chief Deputy Clerk Scott Krahling, Election Staff Coordinator Janice Giron, and staff from the Internet Technology department at Doña Ana County. Clerk's Office representatives provided detailed descriptions of policies related to collecting, using and preserving documents containing private information. The IT department helped address areas of concern related to county IT practices and capabilities.

The committee finds that given the legal requirements of the office it is impossible to reduce the risk to zero. The Clerk's Office has taken several steps to substantially reduce the risk, and if additional recommendations are implemented by the County Clerk and the New Mexico Secretary of State, we believe the risk will be as close to zero as possible.

The following report is a summary of ERC recommendations to reduce the risk of a security breech involving personal private information collected in the County Clerk's Office. It is organized into four sections: internal department practices, internal county practices, state database recommendations, and public assistance.

I. Internal Department Practices

This section outlines suggestions related to the practices and policies governing the work being conducted by staff in the County Clerk's Office.

Working Hours

There are two divisions in the Clerk's Office: the Bureau of Elections and Recording & Filing. Each division is broken down into additional two separate teams. In the Bureau of Elections there are the External Relations Team and the Registration Team. In Recording & Filing there are the Records & Licensing Team and the Indexing and Maintenance Team. See Appendix B for the organizational chart outlining the leadership structure.

Prior to the establishment of this committee, employees in the Clerk's Office were allowed, upon approval, to come in early or stay late to work on projects that involved protected personal information. There was no formal rule related to these decisions and most requests were approved regardless of the presence of a member of the leadership team being present.

The Clerk's Office has implemented a new off-hours policy. If an employee needs to work outside of regular hours, he or she must first get approval from the Clerk or Chief Deputy to work on a specific project and report back on the progress made during that time. In addition, a member of the leadership team is required to be present at all times that employees are working outside of regular hours.

We recommend adding a formal employee policy as follows:

> Employees are not allowed to work in the office outside of regular office hours unless approval is granted by the County Clerk or Chief Deputy Clerk and a member of the leadership team is present. The specific member of the leadership team required to be present depends on which department is involved. For Bureau of Elections projects presence is required by one of the following: the Supervisor of Elections, Election Staff Coordinator, External Relations Lead or the Registration Lead. For Recording and Filing projects presence is required by one of the following: the Recording and Filing Supervisor, Records & Licensing Lead or Indexing and Maintenance Lead. Exceptions to the leadership member requirement can be made by the Clerk or Chief Deputy Clerk if Leads in opposite divisions have been cross trained and are able to help address questions related to the project. In addition, if an employee needs access to his or her work space because something is left in the office (such as a phone charger or other personal item), approval must be obtained from the Clerk or Chief Deputy Clerk before going into the office.

Access to Sensitive Information

Prior to the establishment of this committee, employees in the Bureau of Elections had access to Social Security numbers and full dates of birth in paper records and through several reporting functions in the voter-registration electronic database. Employees in the Bureau of Elections are required to access these records to perform daily tasks.

The Clerk's Office has implemented a new practice that reduces access to the paper voter registration records. The Registration Lead's work station is next to the file. During off hours, it is the responsibility of the Recording Lead or Election Staff Coordinator (or other member of the leadership team in their absence) to unlock/lock the voter registration storage files. No lower-level employees have access to the key to this file, which is stored in a password-protected box. While standard practice had always been to lock this storage file overnight, it was not a practice to keep the key secured in a location with limited access. This allowed staff to work on projects involving the paper records outside of normal office hours when a member of the leadership team was not present, a practice that is no longer allowed in the office.

The Voter Registration Electronic Management System (VREMS) is managed by the New Mexico Secretary of State's office. Thus, the Doña Ana County Clerk's Office is not authorized to make decisions and/or policies regarding updates to the system. However, immediately after being informed of the accusations involving identity theft in Doña Ana County, the Clerk's Office worked with the state vendor who was able to provide an option to mask SSNs from search results' screens. We believe these were the screens that were being used by the accused to quickly hand write four or five names per day. It needs to be noted that this option, while a good temporary solution, is not the long-term solution, which will require updates to the programming and also a method by which scanned images with SSNs are rendered inaccessible. Long-term solutions to the issues with VREMS are discussed in Section III, below.

In our opinion, the Clerk's Office has reduced the level of risk to the lowest possible level. Access to the paper records is more secure and the office has taken substantial steps to reduce access to the electronic database while still allowing the critical work of the office to continue without interruption. Supervisors should also be tasked with performing weekly audits of the work being done using the electronic databases. This will require the cooperation of vendors and the implementation of recommendations to the New Mexico Secretary of State as set forth below.

There are other recommendations for reducing risk in the electronic database that are described in the section pertaining to the recommendations being forwarded to the Secretary of State.

Other suggestions for improving access security are set forth in Appendix C.

Investing in Staff

Based upon conversations between the Clerk's Office and those listed in Appendix C, we believe staff in the County Clerk's Office should follow the same standard practices used by the banking and hospital industries, which shall be achieved through the implementation of annual compliance training. This training reinforces the importance of ethics, protecting private information, following the laws related to a secure workplace, and preventing one's self from being misled by a colleague. Considering that the Clerk's Office has access to similar private information, we recommend developing and implementing an annual compliance training associated with each employee's annual evaluation. This training will need to address laws related to personal private information, ethical practices within the office, notary rules and responsibilities, and tests to ensure that the concepts are understood. Each employee should be

required to sign an annual confidentiality acknowledgement during the evaluation. Notary staff should also undergo annual notary training and sign an acknowledgement of the laws.

In addition to the annual training, regular office meetings should be held that deal specifically with issues related to compliance and privacy laws.

The County Clerk's Office has begun working with a consultant to develop the unique compliance training outlined above. The office anticipates that it will be completed and ready to implement before the end of the current fiscal year. In addition, the office has developed a confidentiality acknowledgement and is including it in the staff evaluations being conducted in September. Notary staff has been put through a training course conducted by the Notary Law Institute. The practice is to have this training on an annual basis.

Change Office Layout

Most employees have individualized work stations. At most, two employees share cubicle space. This provides employees with privacy, but it also gives them the opportunity to work on projects without much observation by their colleagues. However, we feel that reducing the risk to the lowest level requires that the layout remain open, giving employees the ability to see one another and one another's work. It will also help implement a potential authorization process that requires two employees to login into certain sections of the VREMS in order to access private information.

The County Clerk's Office has also been working with the County's IT Department to upgrade its video surveillance and workplace-monitoring system. The Clerk's Office has a separate system using different equipment than the rest of the county. We recommend that the Clerk's Office replace its system by utilizing the county's system. The office should also add or reposition a camera to record the space in front of the paper voter-registration file.

II. Internal County Practices

Standard practice in private companies that collect personal private information is to ensure that new staff has passed a criminal background check and credit check. If the county is not currently doing this for staff in the Clerk's Office, we recommend doing so. In addition, updates are done on both criminal and credit checks to identify potential increased security risks. We feel that the staff in the Clerk's Office has access to information requiring a higher level of scrutiny than other staff in the county.

III. State Database Recommendations

The New Mexico Secretary of State's office is developing a new Voter Registration Electronic Management System (VREMS). While the Secretary of State has made significant improvements, the existing system is lacking when it comes to auditing functions for tracking employee actions within the system and tracking actions related to specific records. These types of auditing functions are common in both private and public industries. The existing system also lacks advanced account administration permissions. The system does have built-in permissions, but they are limited. We recommend that the SOS include the following functions in the new software:

- Implement permission requirements for account access.
- Access to scanned images of registration forms should be locally controlled by an administrator.
- Employees should be limited to accessing only that information available to the public unless allowed further access on an as-needed basis by office administrators, i.e., full date of birth, and SSN.
- Increase auditing capacity to view every action taken by staff when logged in.
- Increase auditing capacity to view every action taken related to a specific record.
- Provide for automatic notifications of suspicious activities.

Pending the installation of the new Voter Registration Electronic Management System – which is not scheduled to occur until after the 2016 General Election – Bureau of Elections employees can still access electronic images of voter registration cards containing the voter's Social Security number. In conversations between the Clerk's Office and the vendor of the current system, it was learned that a state-wide program adjustment can be made to the current system to block such access unless approved by a supervisor. The Clerk's Office has asked the Secretary of State to query the vendor as to the cost of implementing such an adjustment, and she is presently awaiting a response.

In view of the importance of protecting voter privacy and to set the prospective registrant's mind at ease, together with the many new voter registrations anticipated prior to the next General Election, we strongly recommend that the Secretary of State work with the vendor to implement this program adjustment as soon as possible prior to the implementation of the new system.

Notwithstanding the above, there still remains one additional problem regarding access to Social Security numbers, namely: access to such information by third-party registration agents who accept voter-registration forms containing complete SSNs. We recommend that the Secretary of State take such steps as are necessary to preclude this practice, perhaps by developing a unique form to be used by agents. This form would require only the last four digits of the SSN. Once the form is received by the deadline to register to vote, the County Clerk will take such steps as are necessary to retrieve the full SSN and enter the voter's registration into the database. If staff finds a mismatch on the form, staff would follow the standard practice of returning the card to the voter with a letter explaining how to rectify the situation. If legislation for this proposal is required, it should be sought in the 2016 legislative session.

IV. Public Assistance

The Clerk's Office has been informed by the Doña Ana County Sheriff's Department that it will be notifying all identified victims when the appropriate time comes during its investigation. There is no expectation the County Clerk will be informed as to the identities of those voters whose records were accessed. Inquiries should be directed to the Doña Ana County Sheriff's Department.

Concerned residents may research their credit or visit the local Internal Revenue Service office located at 505 S. Main, Ste 149, Las Cruces, NM 88001.

V. Conclusion

We believe the risk is statewide. If an employee is intent on criminal activity within any County Clerk's Office using the VREMS system, we believe heightened protocols can dissuade that activity. We recommend similar protocols to those in this report be implemented in the state's other County Clerks' Offices. The workload of the Clerk's Office requires its staff to work with this information, and existing state systems do not have the auditing capabilities needed to flag suspicious activities.

Before this committee started its review, the Clerk's Office began the process of reducing access to private information and had the outline of a plan that included better staff training. We believe that if the Clerk's Office implements the suggestions above, it will have acted appropriately to reduce the risk of private information being stolen from the office. In addition, if the Secretary of State's office implements the recommendations related to the existing and new VREMS, and if the state finds a way to limit access to voter-registration agents, the risk will have been greatly reduced across the state.

Appendix A. ERC Committee Biographies

Russell Allen, Chair

Russell Allen is the Vice President of Operations for Allen Theatres, Inc. He is currently Chair of the Board of the Greater Las Cruces Chamber of Commerce, is a current Board member of Leadership New Mexico, is a member of the Association of Commerce and Industry and has served on its executive committee, and has served as Chair of the Doña Ana County Republican Party.

Dr. Paul Deason

Dr. Paul Deason had a career as an Operations Research Analyst and statistician for the Departments of Defense of the US and UK. He has degrees from the University of California, New Mexico State University, and the US Air War College. Currently, he is President of Science Technology Analysis Team, LLC and Vice President of the InfraGard El Paso Members Alliance and the High Tech Consortium of Southern New Mexico. He is a consulting analyst in economic development, homeland security, and emergency preparation.

Gwendolyn Hanson

Gwendolyn (Gwen) Hanson is President of the League of Women Voters of Greater Las Cruces (2015-2017). She earned her undergraduate degree in Sociology from the University of Houston and her Master's degree in social work from the University of Houston Graduate School of Social Work. As a licensed social worker Ms. Hanson has 20 years of experience in the mental health field, including inpatient/outpatient treatment settings, prevention/intervention in a large suburban school district, as well as being a federal grant manager.

John Hummer

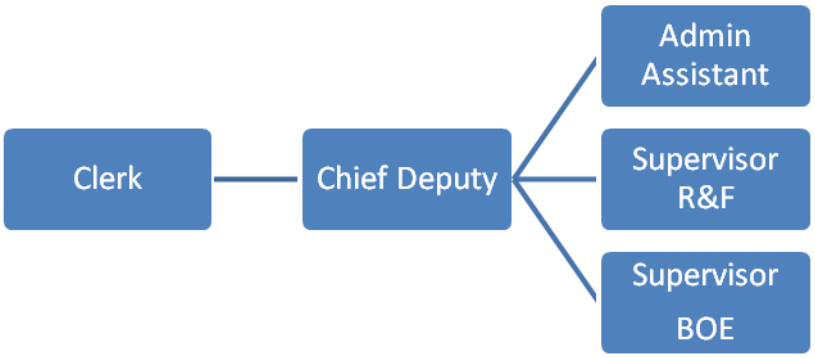
John Hummer is a local businessman and healthcare executive. He was the developer and founding CEO of MountainView Regional Medical Center. He and his wife Amy own Steinborn Inc. Real Estate and he is also the co-founder, executive board member & CEO of the Burrell College of Osteopathic Medicine at NMSU. Prior to coming to Las Cruces in July 2000, John led hospitals as CEO across the country.

John Muñoz

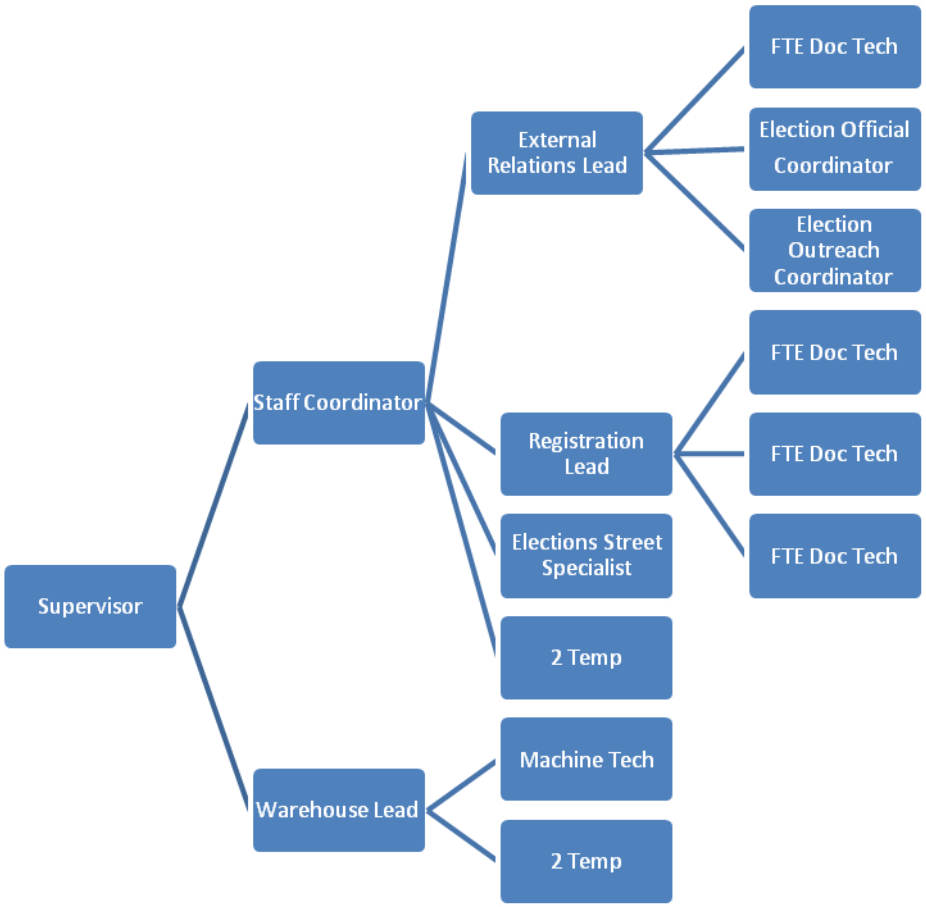
Internationally recognized for his community and philanthropic involvement, John Muñoz leads SiTel-Las Cruces which is one of the larger employers in Dona Ana County. This multi-million dollar organization has seen significant growth year over year. Muñoz is involved with various organizations and sits on several boards, has been a commencement key note speaker for the Las Cruces Public Schools district, and was previously named a "Mover and Shaker" in Southern New Mexico by the *Las Cruces Sun News* and received a White House invitation and recognition as a Champion of Change. Previously Munoz served as Chair of the Hispano Chamber of Commerce and was invited to the Italian Regional Chamber of Commerce in Sassari, Italy. Muñoz speaks Spanish, Italian, and English. Additionally John serves on the Board of Governors as the Chair of the New America School and the Chair-elect of Medical Memorial Board of Trustees.

Appendix B. Office Organizational Chart

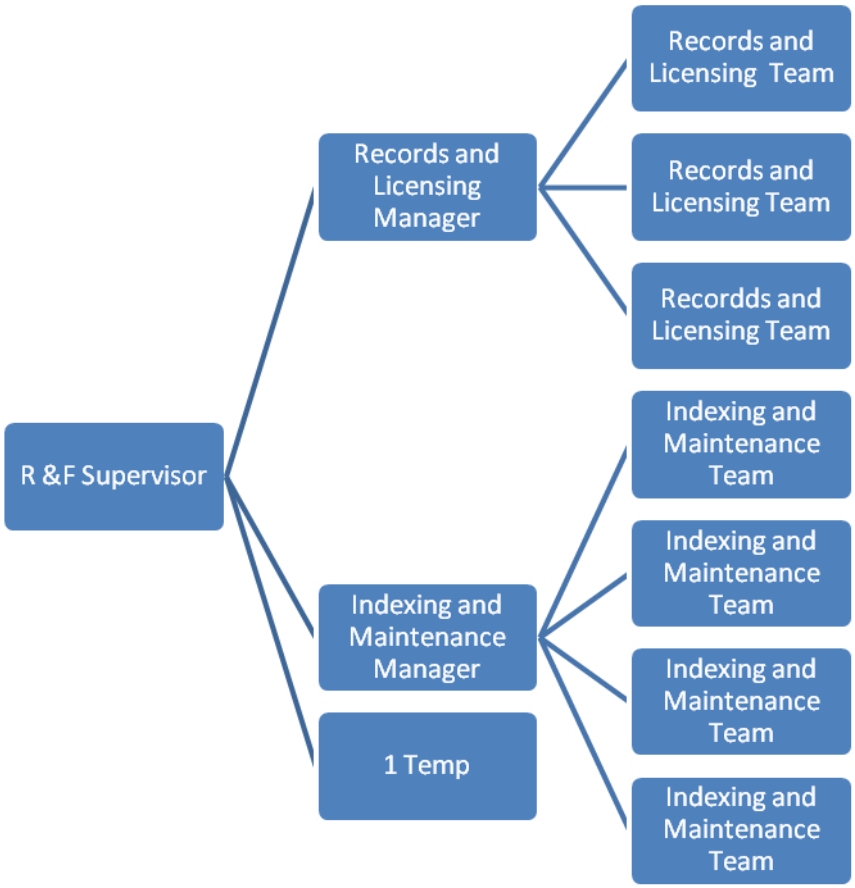
Office Leadership:



Bureau of Elections:



Recording & Filing:



Appendix C. Research Notes

Mountain View Hospital – Mary Noebels, Director of Health Information Management.

Compliance Training as a part of annual evaluations.

Privacy, ethics, and compliance with laws related to protecting information.

Regular privacy reminders during regular meetings.

Database enhancements.

New auditing standards:

Log of date/time of access, screen name, accounts accessed/viewed, search by record and account accessed, search by date ranges, automatic report of suspicious activity, regular reports automatically generated by user, only allow staff to see last 4 digits of SSN, reduce access to scanned images.

Integrity agreement.

Offer 1 year of credit monitoring to victims.

First American Bank – Tim Altamirano, Senior Vice President, Treasury Management.

Database enhancements.

We need to be able to lookup every record and see any activity associated with it. ("see every keystroke").

We need better control over permissions such as preventing people from viewing scanned images, SSNs, full dates of birth, etc.

We need daily reports of anomalies. Suspicious behavior needs immediate notification.

We need to have one person in charge of reviewing reports for suspicious activity.

We should have dual control over access to SSNs.

We should have people from outside government review the new SOS system.