Declaration of Clay U. Parikh

I, CLAY U. PARIKH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and would testify competently to them if called upon to do so.

2. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and continually maintained good standing, until I released it on 28 February 2024. I also held the following certifications: Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

3. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority to Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System Security Manager (ISSM) team for cloud projects. I also have performed numerous internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office (TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing

validated threat CNO penetration testing and systems security analysis. TCNOT is the highest level of implementation of the CNO Team concept.

4. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS) and Pro V&V. My duties were to perform security tests on vendor voting systems for the certification of those systems by either the Election Assistance Commission (EAC), or to a state's specific Secretary of State's requirements.

5. I have provided consultation and technical analysis on several Georgia election complaints and inquiries. In that effort I have reviewed voting system certification test reports, test plans, EAC relevant documents, and Georgia election laws and regulations.

6. While conducting analysis of several Dominion election databases, from various states, I obtained four Georgia county databases from the 2020 election. These databases had originally been obtained via Public Records Requests. The counties were Appling, Bibb, Jones, and Telfair.

7. The focus of that effort was to compare Arizona's election database to other Dominion databases in, Colorado, Georgia, Michigan, and Pennsylvania in preparation for my declaration to the U.S. Supreme Court. The scope of this effort was to further examine the Georgia databases.

EXECUTIVE SUMMARY

8. An ***egregious*** security violation has been discovered, relating to the cryptographic encryption keys utilized by the voting equipment provided and serviced by Dominion Voting Systems, Inc. ("Dominion"). Dominion placed these encryption keys on voting system election databases unprotected and in plain text in violation of EAC-certification requirements and its contract with the state of Georgia. Analysis of the four counties election databases (Appling, Bibb, Jones, and Telfair) confirmed this security violation.

9. The secret encryption key and x509 certificate used to encrypt, decrypt, the election

data, and used for authentication when transferring files and communication are stored in plaintext, unprotected within the election database. Compounding this, the database is not configured to standard security configurations used for a database dealing with sensitive information. These findings indicate that all cryptographic safeguards, designed to ensure the security and accuracy of election results and data, have been rendered meaningless.

10. Upon analysis and review of the four Georgia databases, each database contained simple and easy to guess passcodes, common or shared passwords were also discovered. One anomaly found was that the same exact security code was being utilized in other states during the same election period. The same password and/or security code for certain accounts are identical to the password or security code used in Maricopa County, AZ and Mesa County, CO.

11. Given my education, experience as a security professional and years of experience working with Voting System Testing Laboratories (VSTL), and the thorough analysis of the systems, processes, and the electronic records detailed above, the facts have led to the conclusion that the voters of Georgia should have no confidence that their votes have been accurately counted, if they were even counted at all.

DETAILED FINDINGS AND CONCLUSIONS

12. Dominion's Democracy Suite systems use a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and to authenticate data. The encryption key is considered a secret key and should be hidden and protected. All the components listed above (security processes) should be stored encrypted, especially if stored within a database. In the Democracy Suite systems, they are not. They are left unprotected and out in the open easy to find. See the figures for each county in **Exhibit A**.

13. The purpose of using encryption in election systems is to prevent unauthorized access to those systems and to prevent malicious alteration of election results. EAC-certification requirements mandate that these encryption keys must be kept secret from unauthorized access.

With these items anyone could manipulate system configuration files causing the tabulators to not function properly. They could create or duplicate election data and make it look authentic. The possible attacks or manipulation of data are endless.

14. Furthermore, the plaintext storage of passwords and encryption keys on **any** information system, let alone a voting system, is an **egregious**, **inexcusable** violation of long-standing, **basic** cybersecurity best practices. It destroys any type of security the system wishes to implement. Windows log-in is the only authentication needed to access the unprotected database where the keys are stored.

15. Electronic voting systems overall are full of vulnerabilities with multiple exploits available. The vulnerabilities range from outdated Operating Systems (OS), third party applications, to protocols and services. Adding to these weaknesses is system configuration. Nearly all aspects of the voting systems do not use standard security, let alone industry best practices when configuring their systems. Voting system vendors, like Dominion, lack basic configuration management of their systems. Windows log-in can easily be bypassed.[1]

16. The election database is a prime example of misconfiguration. It is standard practice for a database to not use OS authentication to access or modify the database. Democracy Suite versions use OS authentication, which increases the number of attack vectors on the database. Additionally, if a database is to hold sensitive data it should be configured to encrypt the table, column, or row to which the sensitive data is to reside. This prevents anyone with read only or unauthorized access from seeing the data.

17. These keys being plaintext outside of the cryptographic module also **violates** FIPS 140-2. Section 4.7 of FIPS 140-2 "Cryptographic Key Management"[2] states "The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys[.]" The section also states that "Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution." Section 4.7.5 "Key Storage" states "Plaintext secret and private keys shall not be accessible from

[1] https://www.youtube.com/watch?v=2v-mGf4_9-A
[2] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf pg.30

outside the cryptographic module to unauthorized operators." Additionally, the National Institute of Standards and Technology NIST SP 800-57[3] section 4.7 "Key Information Storage" states "The integrity of all key information **shall** be protected; the confidentiality of secret and private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]"

18. Georgia law requires that the voting system be certified by the EAC. O.C.G.A. § 21-2-300 (2022). The EAC requires voting systems to be tested for compliance with the Voluntary Voting Systems Guidelines (VVSG). The VVSG specifically include requirements for storing cryptographic encryption keys, expressly adopting the Federal Information Processing Standards (FIPS) defining the mandatory practices and management of these keys to include storage of the keys in a cryptographic module or to be encrypted themselves.[4]

19. Of additional note regarding the technical and supervisor passcodes, the string of numbers repetitively used as a passcode in the Georgia voting systems was also the same **exact** passcode found and used in both Maricopa County, Arizona and Mesa County, Colorado. This commonly known, easy to guess passcode, which was used across multiple states, increases the risk of possible exploitation exponentially.

20. Another anomaly like the one mentioned above also exists with some of the administrative account passwords and security codes. The Georgia accounts either share the same password, security code or both with Maricopa and Mesa County. *See* figures B-1 and B-2 in **Exhibit B**. The blue arrows on these figures highlight the out of state counties that have the same credentials. This is highly suspicious but more importantly it is a security concern.

21. I reviewed Dominion's response to these revelations.[5] Dominion's statement that "*The claim that access to any single credential could affect the result of an election undetected is implausible and conspiratorial*" is misleading for three reasons:

[3] https://doi.org/10.6028/NIST.SP.800-57pt2r1
[4] VVSG 1.0 (2005) 7.4.5.1 https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF
[5] https://lawandcrime.com/supreme-court/kari-lake-to-scotus-hurry-up-the-2024-election-is-coming-and-dominion-voting-machines-need-to-be-banned/

- While access to a "single credential" as characterized by Dominion, would likely not be sufficient to manipulate an election, that is not the situation here. The Dominion voting systems are so ill configured and full of vulnerabilities that one single user credential could gain access to the database where the encryption keys are left unprotected and in plain text for the world to see.
- Access to these unprotected in plain text encryption keys provide the capability to unlock or manipulate other accounts.
- Lastly, the encryption keys provide the means with which to fabricate and/or manipulate election results, change the configuration of voting systems components such as the tabulator. Manipulation of election results could happen at any level; the tabulator, memory card, server, or database level, which would be accepted by the system as authenticated results.

22. Dominion's statement that "*Dominion's machines are fully certified by the U.S. Election Assistance Commission...*" is likewise misleading because EAC certification of a voting system is not strictly limited to its operation "as tested" and defined in the corresponding Scope of Conformance. EAC-certification is an operational standard which must be maintained within the specifications as defined in the VVSG throughout the use of the voting system. *See, e.g.,* VVSG Sections 8.1 (discussing the conforming the system to meet VVSG and state and local requirements throughout the life of the system) and 9.5 (discussing establishment of procedures to resolve identified defects). Dominion's voting systems are not operating as tested and certified by the EAC.

23. Dominion is also not compliant with its contract with the state of Georgia for the reasons previously stated in this declaration concerning the encryption keys. Exhibit B to the Master Solution Purchase and Services Agreement Dominion states:

- Section 8. System Security Description "Dominion utilizes authentication and authorization protocols that meet EAC VVSG 2005 standards. In addition, Dominion's solution relies on industry-standard security features to ensure that the

correct users based on a user role or group are granted the correct privileges."

- Section 8.3 Encryption configurations for both data at rest and data in motion "Data generated by the Democracy Suite platform is protected by the deployment of FIPS approved symmetric AES and asymmetric RSA encryption."
- Section 8.9 Secure Development Process "Data integrity and confidentiality is also implemented according to NIST defined and FIPS validate procedures and algorithms."

None of these sections are being fulfilled with the voting system in its current state.

CONCLUSION

24. The analysis of the four Georgia county databases, the multitude of account and credential issues found, the numerous vulnerabilities associated with the voting system components leave the voting systems in Georgia lacking any system integrity. The encryption mechanisms and security certificates are left totally unprotected in a highly vulnerable system in violation of the VVSG and EAC certification requirements. The result of these critical faults, individually or collectively, means there is no way to know if votes cast in either 2020 or 2022 election were correctly recorded or tabulated. Also, as there is no evidence these issues and violations have been resolved, there is no way to know if the results for the 2024 election cycle will be correctly recorded or tabulated.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 7th day of August 2024.

s/ Clay Parikh
Clay U. Parikh

Exhibit A

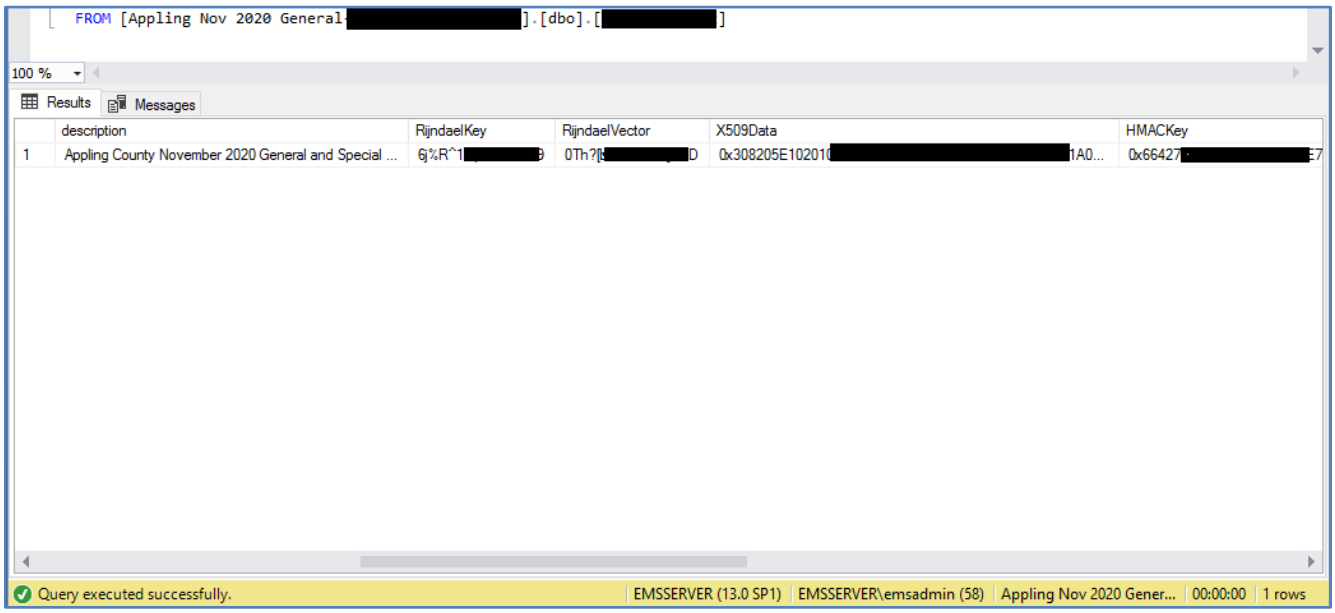

Figure A-1. Appling encryption keys

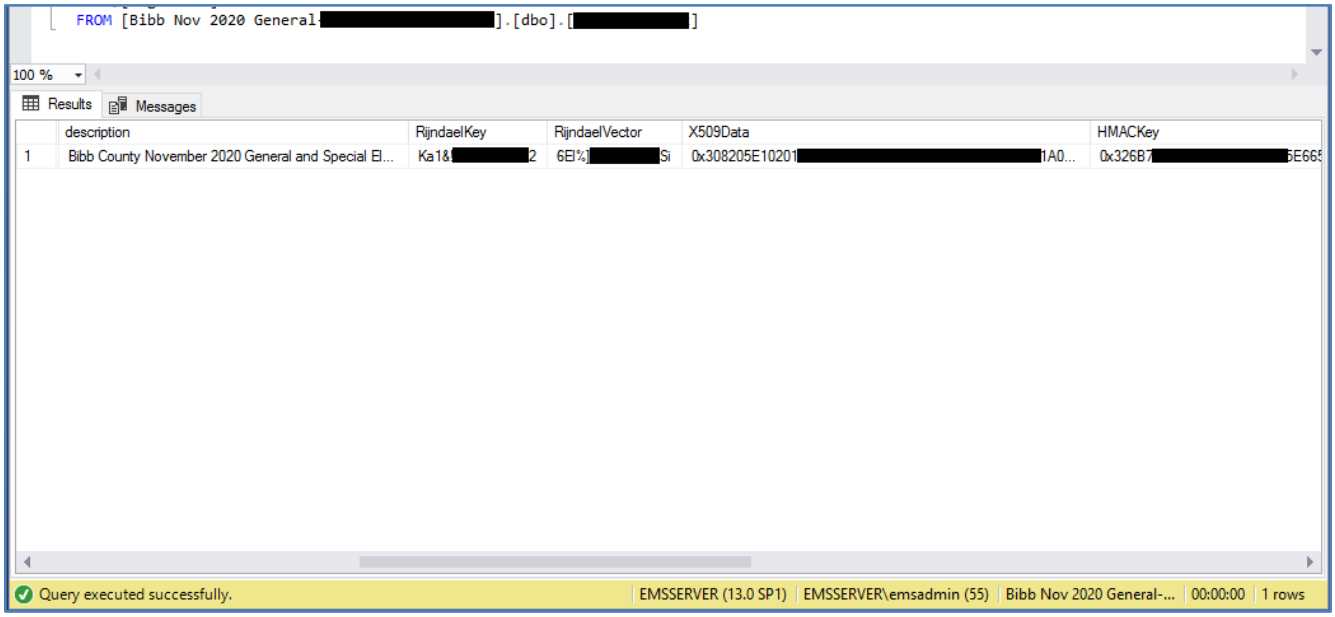

Figure A-2. Bibb encryption keys

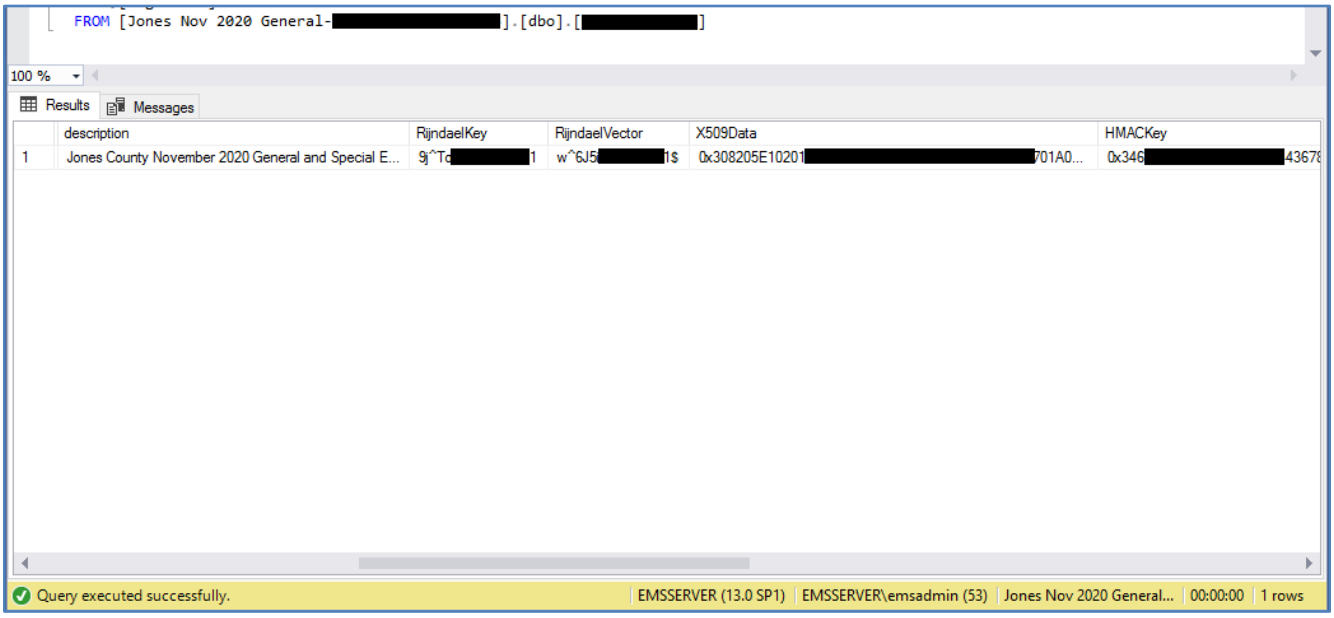

Figure A-3. Jones encryption keys

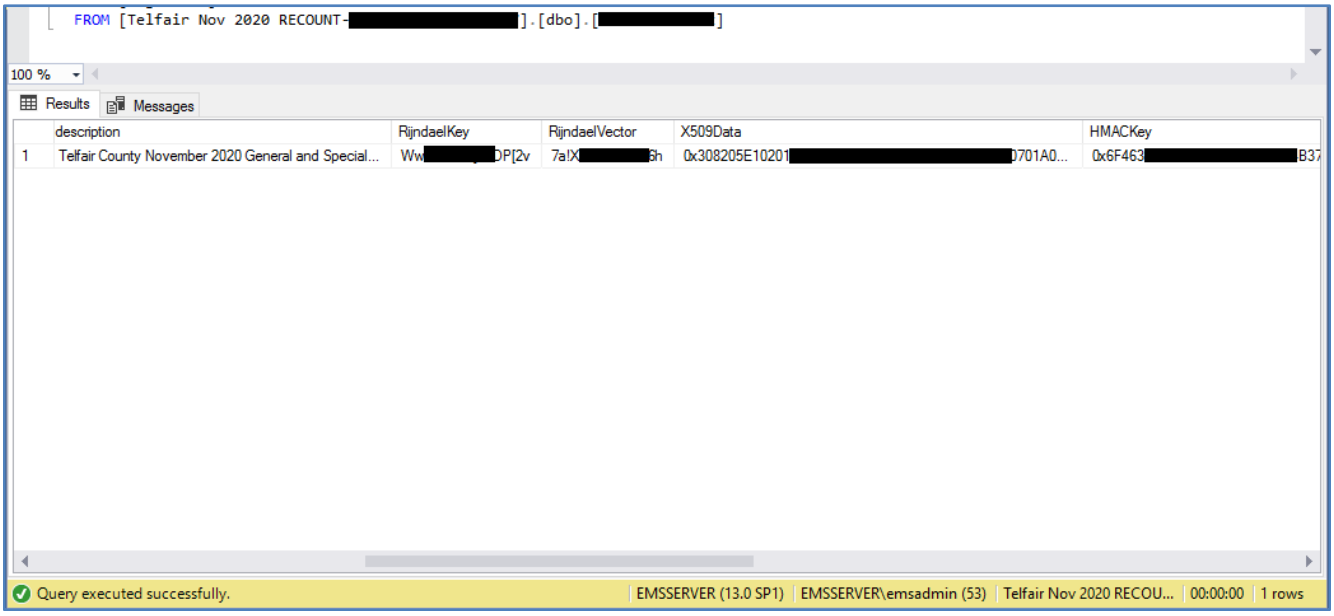

Figure A-4. Telfair encryption keys

Exhibit B

username	password	firstName	lastName	County
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Appling
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Appling
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Appling
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Bibb
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Bibb
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Bibb
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Jones
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Jones
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Jones
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Telfair
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Telfair
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Telfair
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith	Maricopa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Maricopa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Maricopa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Maricopa
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith	Mesa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Mesa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Mesa
Admin	0x6166A73[redacted]CEF986384	John	Smith	Mesa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Mesa
RTRAdmin	0x6166A73[redacted]CEF986384			Mesa

Figure B-1. Common Passwords

username	password	firstName	lastName	__securitycode	County
Techadvisor	0xC97922[redacted]A6A2EF52	State of	Georgia	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Appling
Admin	0xC97922[redacted]A6A2EF52	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Appling
Techadvisor	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Bibb
Admin	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Bibb
Techadvisor	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Jones
Admin	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Jones
Techadvisor	0x08A131[redacted]A8319A7B	State of	Georgia	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Telfair
Admin	0x08A131[redacted]A8319A7B	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Telfair
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Maricopa
Admin	0x7058D7[redacted]3E5984C2B	Bruce	Hoenicke	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Maricopa
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]HNFOMHVSRrGxg+a	Mesa
Admin	0x6166A7[redacted]EF986384	John	Smith	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Mesa

Figure B-2. Common Security Codes