June 15, 2023

JASON PROVIDAKES, PH.D.,
President & Chief Executive Officer, MITRE

Dear Dr. Providakes:

We are researchers and academics who are recognized experts in the fields of cybersecurity and election security. We are writing to call your attention to an unsigned report written by the MITRE National Election Security Laboratory (NESL) entitled “Independent Technical Review: Security Analysis of Georgia’s ImageCast X Ballot Marking Devices”, and to urge MITRE to retract this report.

This report was commissioned by Dominion Voting Systems in March 2022 and was recently unsealed by the U.S. District Court for the Northern District of Georgia in the matter of *Curling v. Raffensperger*.[1] Dominion hired MITRE to write the report in response to vulnerabilities in Georgia’s Dominion voting equipment that were discovered by Prof. J. Alex Halderman of the University of Michigan and Prof. Drew Springall of Auburn University while performing court-authorized security testing for the *Curling* plaintiffs.[2] Their findings were confirmed by CISA, which issued a security advisory about the vulnerabilities in June 2022.[3] Dominion has developed updated firmware (Democracy Suite 5.17) that purportedly addresses some of these vulnerabilities.

Unlike Halderman and Springall, MITRE NESL was not provided access to Dominion’s equipment and did not perform any security testing. Instead, MITRE attempted to assess the risk posed by potential attacks described in Halderman and Springall’s expert report without essential access to the source information.

MITRE’s analysis applies faulty reasoning and dangerously understates the risk of exploitation, asserting that the attacks would be “operationally infeasible.” This contradicts CISA's determination that “these vulnerabilities present risks that should be mitigated as soon as possible.” MITRE's logic is that *if* procedural defenses are perfectly implemented, *then* the system is immune from attack. This is a completely inappropriate methodology for assessing real-world risk, since actual risk hinges on how well defenses are implemented and operate in practice.

[1] MITRE, “Independent Technical Review: Security Analysis of Georgia’s ImageCast X Ballot Marking Devices” (July 2022). Available at https://www.dominionvoting.com/mitre-report/.

[2] J. Alex Halderman and Drew Springall, “Security Analysis of Georgia’s ImageCast X Ballot Marking Devices”, Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al., *Curling v. Raffensperger*, Civil Action No. 1:17-CV-2989-AT U.S. District Court for the Northern District of Georgia, Atlanta Division (July 1, 2021). Available at https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1681.0.pdf.

[3] CISA, “ICS Advisory ICSA-22-154-01: Vulnerabilities Affecting Dominion Voting Systems ImageCast X” (June 3, 2022). Available at https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01.

MITRE's entire analysis is predicated on an assumption known to be wrong. As noted on the first page of the document, "MITRE's assessment of the researcher's proposed attacks **assumes strict and effective controlled access** to Dominion election hardware and software." That assumption was ill-considered when it was written, and it is ridiculous today, since we now know that the Georgia Dominion software has *already been stolen and widely distributed*[4] and that election equipment in at least one Georgia county was repeatedly improperly accessed.[5] In Coffee County, Georgia, the Dominion equipment was "stored in a room with an unlocked door to the outside of the building, a leaking roof, and walls with sunlight streaming through crevices."[6] Yet MITRE's risk assessment assumes that Georgia perfectly protects the equipment from illicit access across all of its 159 counties.

The lapses that have already occurred in Georgia would be sufficient to let malicious parties develop and test attacks that exploit the vulnerabilities Halderman and Springall discovered, and potentially other vulnerabilities that they missed.

MITRE's analysis isn't simply wrong—it is dangerous, since it will surely lead states like Georgia to postpone installing Dominion's software updates and implementing other important mitigations. Georgia Secretary of State Brad Raffensperger recently announced that he will forgo installing Dominion's security patches until after the 2024 presidential election, no doubt acting in reliance on MITRE's misleading risk assessment. This announcement gives potential adversaries nearly 18 months to prepare to exploit the flaws against real elections in the state.

More than 16 other states use the same Dominion equipment, including other likely swing states such as Nevada, Arizona, and Michigan. They too must decide whether to remedy the flaws or to ignore them as "operationally infeasible" based on MITRE's advice. If the now-public vulnerabilities are exploited to disrupt or discredit elections in 2024, MITRE will share responsibility for this entirely preventable security failing.

Security risks have to be assessed empirically, based on the effectiveness of defenses as they are actually practiced—not based on some idealized conception of those defenses. In light of the overwhelming evidence of physical security lapses in Georgia and other states, **MITRE should immediately retract its analysis**, which fails to account for the real-world conditions under which election equipment is stored and operated and for deficiencies in Georgia's election audits. If MITRE's faulty assumptions are corrected, its own reasoning will lead to the opposite (and correct) conclusion: Halderman and Springall's attacks pose a "scalable" threat to the integrity of U.S. elections, and states should urgently mitigate them.

If MITRE genuinely aspires to "provide objective analysis" about election systems, it will correct the record now and retract its dangerously misleading analysis.

[4] https://www.washingtonpost.com/investigations/2022/10/28/coffee-county-election-voting-machines/
[5] https://www.washingtonpost.com/investigations/2022/10/28/coffee-county-georgia-voting-trump/
[6] Memo from James Barnes, former election supervisor for Coffee County, Georgia to the Georgia Secretary of State's office, Aug. 24, 2021, available at: https://coaltionforgoodgovernance.sharefile.com/share/view/s97b6525eb8ea45518b58d5c64a825abd

Sincerely,[7]

Josh Aas, Executive Director, Internet Security Research Group

Mustaque Ahamad, Professor, School of Cybersecurity and Privacy, Georgia Institute of Technology

Andrew W. Appel, Eugene Higgins Professor of Computer Science, Princeton University

Duncan A. Buell, Chair Emeritus, NCR Chair in Computer Science and Engineering, University of South Carolina, Columbia

Richard DeMillo, Professor and Charlotte B and Roger C Warren Chair in Computing, Georgia Tech, Atlanta GA

Zakir Durumeric, Assistant Professor of Computer Science, Stanford University

Aleksander Essex, Associate Professor of Software Engineering, Western University, Canada

Michael J. Fischer, Professor of Computer Science, Yale University

Robert Graham, cybersecurity expert

Matthew D. Green, Associate Professor of Computer Science, Johns Hopkins University

Harri Hursti, independent security researcher, co-founder Voting Village @ DEF CON

David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory (retired)

Douglas W. Jones, Emeritus Associate Professor of Computer Science, University of Iowa

Joseph Kiniry, Principal Scientist - Galois & CEO and Chief Scientist - Free & Fair

Patrick McDaniel, Tsun-Ming Shih Professor of Computer Sciences, University of Wisconsin-Madison

Prateek Mittal, Professor, Princeton University, Interim Director, Center for Information Technology Policy (CITP)

Olivier Pereira, Professor, UCLouvain

Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology

Peter Y A Ryan, University of Luxembourg

Peter B. Rønne, Chercheur, CNRS, LORIA, France

Bruce Schneier, security technologist and Lecturer, Harvard Kennedy School

E. John Sebes, Chief Technology Officer, OSET Institute

Barbara Simons, Computer Scientist, IBM Research (retired)

Kevin Skoglund, Chief Technologist, Citizens for Better Elections

Eugene H. Spafford, Professor, Executive Director Emeritus, CERIAS, Purdue University

Michael Alan Specter, PhD, Security Researcher

Philip B. Stark, Distinguished Professor of Statistics, University of California, Berkeley

Vanessa Teague, CEO, Thinking Cybersecurity Pty Ltd and Associate Professor (Adj.), The Australian National University

Poorvi L. Vora, Professor of Computer Science, The George Washington University

[7] Affiliations are listed for identification purposes only and do not indicate endorsement by the institutions mentioned therein.