MITRE

MP220250
MITRE PRODUCT

Independent Technical Review: *Security Analysis of Georgia's ImageCast X Ballot Marking Devices*

July 2022

McLean, VA

Executive Summary

Dominion Voting Systems Corp., via counsel Susman Godfrey, L.L.P., retained MITRE's National Election Security Lab (NESL) to provide an independent expert technical review of claims made by a researcher concerning the security of specific devices used in the conduct of elections in the State of Georgia. On behalf of the plaintiffs in *Curling v. Raffensperger*,[1] the researcher submitted a security analysis of Georgia's ImageCast X (ICX) Ballot Marking Devices (BMDs). These devices, produced by Dominion Voting Systems Corp., are currently distributed state-wide to every electoral precinct and have become the primary mechanism through which Georgia voters make selections and print ballots during elections. In the security analysis, the researcher claims to have exploited vulnerabilities in Georgia's BMDs that "could be effectuated by malicious actors with very limited time and access to the machines" and that it would be possible to commit "large-scale fraud" with "only moderate technical skills."

In this report, as an independent technical reviewer, MITRE NESL undertakes a technical analysis to assess the feasibility of the researcher's proposed attacks to change the outcome of a Georgia election. Without access to Georgia voting equipment or the researcher's proof-of-concept capabilities, MITRE NESL began by assuming validity of the researcher's technical capabilities. The researcher was provided with unrestricted physical access, system documentation, and passcodes for the devices examined. Under these conditions, security researchers may reasonably be assumed capable of compromising a device, regardless of manufacturer. MITRE NESL summarizes and assesses each of the researcher's principal findings, attack capability claims, and main conclusions.

MITRE NESL observed six total attack scenarios hypothesized by the researcher. Four of the proposed attacks involve replacing election software on BMDs with malicious software that alters a ballot before being printed and is disguised to look like Dominion's official application; one attack inserts malicious hardware components into a BMD printer; and one describes a ballot stuffing scenario.

The researcher's proposed attacks were assessed by MITRE NESL to be operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations. Each of the attacks requires access and/or opportunity that remains unavailable in the operational environment. Five of six attacks were deemed non-scalable, impacting a statistically insignificant number of votes on a single device at a time. One attack was technically scalable but also was assessed to be infeasible due to access controls in place in operational election environments, access required to Dominion election software, and access required to Dominion election hardware.[2] Five of the proposed attacks involve modifications to a printed ballot's Quick Response (QR) code—a non-authoritative portion of a Georgia ballot—that can be detected through Risk-Limiting Audits (RLAs).

MITRE NESL has no evidence that any of the researcher's proposed attacks, in whole or in part, have been attempted by any party in an election.

[1] Dominion Voting Systems Corp. is not a party in the referenced litigation.

[2] MITRE's assessment of the researcher's proposed attacks assumes strict and effective controlled access to Dominion election hardware and software.

Table of Contents

1 Introduction

The MITRE Corporation is a not-for-profit company that works in the public interest to help the nation address difficult problems that challenge the safety, stability, security, and well-being of the country. MITRE operates six federally funded research and development centers (FFRDCs), participates in public-private partnerships, and maintains an independent technology research program. Working across federal, state, and local governments—as well as industry and academia—gives MITRE a unique vantage point. MITRE works in the public interest to discover new possibilities, create unexpected opportunities, and lead by pioneering together for public good to bring innovative ideas into existence in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, cyber-physical systems security, trustworthy autonomy, cyber threat sharing, and cyber resilience.

MITRE's National Election Security Lab (NESL) provides state, local, and federal officials, and election industry participants, a means to maintain public trust and confidence in our election systems. Leveraging MITRE's cybersecurity, cyber-physical security, and interdisciplinary analysis expertise, NESL works with partners to provide objective analysis of the security risk management associated with election products, jurisdiction and state comprehensive election systems and procedures, and related services.

1.1 Purpose

On 1 July 2021, a researcher submitted, on behalf of the plaintiffs in *Curling v. Raffensperger*,[3] a security analysis of Georgia's ImageCast X (ICX) Ballot Marking Devices.[4] The researcher was provided with unrestricted access to the devices, documentation, and passcode information for the devices over a period of time that appears to total twelve person-weeks. Pursuant to the research period, the researcher's report asserts an ability to exploit vulnerabilities in the ICX Prime ballot marking device (BMD) in a manner that "could be effectuated by malicious actors with very limited time and access to the machines"[5] and that it would be possible to commit "large-scale fraud"[6] with "only moderate technical skills."[7]

These serious claims have potentially grave consequences to the national election landscape. Dominion Voting Systems Corp., via counsel Susman Godfrey, L.L.P., retained MITRE's National Election Security Lab (NESL) to provide an independent expert technical review of the researcher's claims.

1.2 Scope

This report summarizes the proof-of-concept attacks[8] proposed in the researcher's July 2021 security analysis and assesses the feasibility of each attack changing the outcome of a Georgia

[3] *Curling v. Raffensperger*, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, Atlanta Division.

[4] J. Alex Halderman, *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, 1 July 2021.

[5] ibid., p. 4.

[6] ibid., p. 7.

[7] ibid., p. 7.

[8] A "proof-of-concept" attack is a real but non-harmful attack used to demonstrate security weakness in a system.

election. Because the researcher was provided with unrestricted physical access, documentation, and access codes for the devices in question, the MITRE NESL team adopted an operating assumption that the attacks were technically valid as described.

2 Summary of Claims

The researcher makes multiple claims about the security of the Georgia election system, including that some attacks "could be effectuated by malicious actors with very limited time and access to the machines."[9] The researcher describes seven principal findings[10] (Table 1), four proof-of-concept attacks[11] (Table 2), and six main conclusions[12] (Table 3). Tables 1-3 are MITRE NESL's plain-language interpretations of the researcher's claims. MITRE NESL provides a technical analysis of the claims in Section 5, and assessment of the claims in Section 6.

Table 1. Claimed Principal Findings from the Researcher's Report

No.	Researcher's Principal Findings	MITRE NESL's Plain-Language Summary of Researcher's Claim
PF.1	"Attackers can alter the [Quick Release] QR codes on printed ballots to modify voters' selections. Critically, voters have no practical way to confirm that the QR codes match their intent, but they are the only part of the ballot that the scanners count. I demonstrate how the QR codes can be modified by compromising the BMD printer or by installing malware on the BMD."	**The researcher asserts that with access to a BMD or BMD printer, attackers can tamper with Georgia's voting equipment to change voters' selections within QR codes without their knowledge.**
PF.2	"The software update that Georgia installed in October 2020 left Georgia's BMDs in a state where anyone can install malware with only brief physical access to the machines. I show that this problem can potentially be exploited in the polling place even by non-technical voters."	**The researcher asserts that the process used to update the ICX software on Georgia BMDs in October 2020 left the equipment vulnerable to attack.**
PF.3	"Attackers can forge or manipulate the smart cards that the ICX uses to authenticate technicians, poll workers, and voters. Without needing any secret information, I created a counterfeit technician card that can unlock any ICX in Georgia, allowing anyone with physical access to install malware."	**The researcher asserts that attackers can produce unofficial smart cards[13] or manipulate official cards to create or enable tampering opportunities for attackers with physical access to Georgia BMDs.**
PF.4	"I demonstrate that attackers can execute arbitrary code with root (supervisory) privileges by altering the election definition file that county workers copy to every BMD before each election. Attackers could exploit this to spread malware to all BMDs across a county or the entire state."	**The researcher asserts that the election definition file, installed during election setup, can be exploited to deploy malicious software when installed to potentially all BMDs in a county or state.**

[9] ibid., p. 4.

[10] J. Alex Halderman, *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, 1 July 2021. p. 4

[11] ibid., p. 5

[12] ibid., p. 6

[13] For clarity, MITRE NESL uses the term "unofficial smart cards" to describe system access or voter session activation cards that were created or modified outside of Dominion's formal production process or not authorized by an election superintendent.

PF.5	"The ICX contains numerous unnecessary Android applications, including a Terminal Emulator that provides a "root shell" (a supervisory command interface that overrides access controls). An attacker can alter the BMD's audit logs simply by opening them in the on-screen Text Editor application."	**The researcher asserts that using pre-installed software applications present on a BMD, attackers can gain elevated privileges which facilitate attacks and cover their tracks.**
PF.6	"In a given election, all BMDs and scanners in a county share the same set of cryptographic keys, which are used for authentication and to protect election results on scanner memory cards. An attacker with brief access to a single ICX or a single Poll Worker Card and PIN can obtain the county-wide keys."	**The researcher asserts that a compromised encryption key extracted from a BMD or poll worker card (with knowledge of the card's PIN) can be used to decrypt election materials across a county since the same encryption keys can be used within a Georgia county.**
PF.7	"The ImageCast Precinct (ICP) scanner stores ballot scans in the order they were cast. A dishonest election worker (like that emphasized by the Defendants and their expert ([*name redacted*]) with just brief access to the scanner's memory card could violate ballot secrecy and determine how individual voters voted."	**The researcher asserts that an election official with access to a ballot scanner memory card and an ordered list of voter names for that scanner can map individual voters to their ballot selections.**

Table 2. Claimed Proof-of-Concept Attacks from the Researcher's Report

No.	**Researcher's Proof-of-Concept Attack**	**MITRE NESL's Plain-Language Summary of Researcher's Claim**
POC.1	"An attack that uses malicious hardware hidden inside the BMD's printer to alter the votes on printed ballots."	**The researcher's proof-of-concept (POC) attack involves installing a device in a BMD printer to modify ballots when they are printed.**
POC.2	"Malware that runs on the BMD and alters votes while avoiding hash validation, firmware validation, and logic and accuracy testing."	**The researcher's POC attack involves installing software that changes votes on a printed ballot and circumvents detection on a BMD.**
POC.3	"An automated method of installing malware by briefly unplugging the printer cable and attaching a malicious USB device."	**The researcher's POC attack involves a hardware device that performs automated installation of malicious software when attached to a BMD.**
POC.4	"Vote-stealing malware that can be installed remotely from the [Election Management System] EMS, by altering the BMD's election definition file."	**The researcher's POC attack involves a modified election definition file that installs malicious software when distributed to BMDs.**

Table 3. Claimed Main Conclusions from the Researcher's Report

No.	Researcher's Main Conclusion	MITRE NESL's Plain-Language Summary of Researcher's Claim
MC.1	"The ICX BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia. Adversaries with the necessary sophistication and resources to carry out attacks like those I have shown to be possible include hostile foreign governments such as Russia—which has targeted Georgia's election system in the past—and domestic political actors whose close associates have recently acquired access to the same Dominion equipment that Georgia uses through audits and litigation in other jurisdictions."	**The researcher asserts that BMDs in use by Georgia are susceptible to the proposed attacks and findings. Adversaries can include foreign state and/or domestic political actors with access to Dominion equipment.**
MC.2	"The ICX BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X [Direct Recording Electric voting machines] DREs they replaced. Both systems have similar weaknesses, including readily bypassed user authentication and software validation, and susceptibility to malware that spreads from a central point to machines throughout a jurisdiction. Yet with the BMD, these vulnerabilities tend to be even easier to exploit than on the DRE system, since the ICX uses more modern and modular technology that is simpler to investigate and modify."	**The researcher asserts that BMDs in use by Georgia are not more secure than AccuVote Direct-Recording Electric (DRE) machines. BMDs and the associated ICX software take less time to exploit compared to AccuVote DREs.**
MC.3	"Despite the addition of a paper trail, ICX malware can still change individual votes and most election outcomes without detection. Election results are determined from ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text. Although outcome-changing fraud conducted in this manner could be detected by a risk-limiting audit, Georgia requires a risk-limiting audit of only one contest every two years, so the vast majority of elections and contests have no such assurance. And even the most robust risk-limiting audit can only assess an election outcome; it cannot evaluate whether individual votes counted as intended."	**The researcher asserts that the BMD-printed paper trail provides an opportunity for attackers to change voters' selections within QR codes without their knowledge. The researcher also asserts that these attacks are difficult to detect given Georgia's current risk-limiting audit (RLA) policies and practices.**
MC.4	"The ICX's vulnerabilities also make it possible for an attacker to compromise the auditability of the ballots, by altering both the QR codes and the human readable text. Such cheating could not be detected by an RLA or a hand count, since all records of the voter's intent would be wrong. The only practical way to discover such an attack would be if enough voters reviewed their ballots, noticed the errors, and alerted election officials, and election officials identified the problem as a systemic hack or malfunction; but human-factors studies show that most voters do not review their ballots carefully enough, and election officials likely would consider such reports the product of voter error. This means that in a close contest, ICX malware could manipulate enough ballots to change the election outcome with low probability of detection. In contrast, risk-limiting audits of hand-marked paper ballots, when used with appropriate procedural precautions, provide high confidence that individual votes are counted as intended and election outcomes are correct even if the election technology is fully compromised."	**The researcher asserts that ballot-manipulating attacks can be adapted to change voters' selections in both the QR code and the plaintext portions of a printed BMD ballot. The researcher also asserts that this scenario avoids detection during RLAs. The conclusion relies on voters not reviewing their printed ballots and inconsistencies being attributed to user error.**

No.	Researcher's Main Conclusion	MITRE NESL's Plain-Language Summary of Researcher's Claim
MC.5	"Using vulnerable ICX BMDs for all in-person voters, as Georgia does, greatly magnifies the security risks compared to jurisdictions that use hand-marked paper ballots but provide BMDs to voter upon request. When use of such BMDs is limited to a small fraction of voters, as in most other states, they are a less valuable target and less likely to be attacked at all. Even if they are successfully compromised, attackers can change at most a small fraction of votes—which, again, creates a strong disincentive to undertake the effort and risk to change any such votes."	**The researcher asserts that Georgia assumes an increased risk of attack on its elections with its BMD-only system, where the BMDs are considered vulnerable. The researcher also asserts that other locations that use a combination of hand-marked paper ballots and optional BMDs are less likely to be attacked. BMDs in the latter scenario only print a small number of votes, which reduces attackers' incentives and potential impact.**
MC.6	"The critical vulnerabilities in the ICX—and the wide variety of lesser but still serious security issues—indicate that it was developed without sufficient attention to security during design, software engineering, and testing. The resulting system architecture is brittle; small mistakes can lead to complete exploitation. Likewise, previous security testing efforts as part of federal and state certification processes appear not to have uncovered the critical problems I found. This suggests that either the ICX's vulnerabilities run deep or that earlier testing was superficial. In my professional experience, secure systems tend to result from development and testing processes that integrate careful consideration of security from their inception. In my view, it would be extremely difficult to retrofit security into a system that was not initially produced with such a process."	**The researcher asserts that Dominion's ICX software does not appear to follow modern secure software design principals and will be challenging to retrofit with security features. The researcher also asserts that despite its vulnerabilities, the ICX system was certified by programs that do not seem to be effective.**

3 Georgia Voting Overview

Starting in May 2020, Georgia required use of voter-verifiable paper ballots marked by electronic ballot markers and tabulated by ballot scanners.[14,15] In 2019-2020, Georgia purchased 33,100 BMDs and 3,800 ICP Tabulators[16] from Dominion to replace its previous system.[17] The state aimed to distribute 31,826 BMDs to its 159 counties to ensure each county had at least one BMD per 225 active voters.[18] By law, Georgia requires one voting booth or enclosure per 250 voters in a precinct.[19] There were 2,656 precincts in the Georgia 2020 General Election.[20]

[14] Ga. Comp. R. & Regs.183-1-12-.01. Retrieved 17 June 2022 from https://rules.sos.state.ga.us/gac/183-1-12.

[15] Ga. Code Ann. § 21-2-379.22. Retrieved 17 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-9-voting-machines-and-vote-recorders-generally/part-6-electronic-ballot-markers/section-21-2-37922-requirements-for-electronic-ballot-marking

[16] Georgia Secretary of State, Dominion Contract Amendment 1. Retrieved 17 June 2022 from https://web.archive.org/web/20210819043116/https://sos.ga.gov/admin/uploads/Dominion_Contract-_Amendment_1-_Executed.pdf

[17] Georgia Department of Administrative Services, *New Voting System - Request for Information*. Retrieved 22 June 2022 from https://ssl.doas.state.ga.us/PRSapp/PublicBidNotice?bid_op=194780047800-SOS0000035

[18] Stephen Fowler, *Georgia Buying More New Voting Machines for Counties Ahead Of 2020 Rollout*, December 16, 2019. Retrieved 25 May 2022 from https://www.gpb.org/news/2019/12/16/georgia-buying-more-new-voting-machines-for-counties-ahead-of-2020-rollout

[19] Ga. Code Ann. § 21-2-367. Retrieved 06 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-9-voting-machines-and-vote-recorders-generally/part-4-optical-scanning-voting-systems/section-21-2-367-installation-of-systems-number-of-systems-good-working-order

[20] Georgia Secretary of State, *November 3, 2020 General Election Results*. Retrieved 09 June 2020 from https://results.enr.clarityelections.com/GA/105369/web.264614/#/summary.

The 2020 Georgia General Election consisted of 4,999,960 total votes for the presidential race.[21,22] 3,682,422 votes were cast in-person, 1,315,294 were cast via mail-in ballot,[23] and 2,244 votes were write-ins with no further information located on casting method.

In-person voting opportunities in the Georgia 2020 General Election spanned roughly 18 days (12 October 2020 – 3 November 2020). Advance voting days on Sundays are optional. Georgia's advance voting begins the fourth Monday before an election and ends the last Friday before the event.[24] During the 2020 advance voting period, approximately 2,694,763 votes were cast in-person.[25]

An official ballot in Georgia is defined as an "instrument, whether paper, mechanical, or electronic, by which an elector casts his or her vote"[26] and is "furnished by the superintendent or governing authority in accordance with Code Section 21-2-280, including paper ballots that are read by ballot scanners."[27] Ballots must contain the text "OFFICIAL BALLOT," precinct information, the name and date of the election, and the statement: 'I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law.'[28]

Paper ballots printed by electronic BMDs "shall be designed as prescribed by the Secretary of State to ensure ease of reading by electors"[29] and shall be "marked with the elector's choices in a format readable by the elector."[30]

A marked ballot in Georgia consists of Georgia-required text and two components containing ballot selections: (1) a QR code; and (2) a plaintext summary.[31] The QR code is a two-dimensional barcode that is scanned and tabulated by ballot scanners. Voters are encouraged to review the plaintext summary by election officials stationed at ballot scanners who are required

---

[21] State of Georgia, *2020 Votes Cast for Certified Write-In Candidates*, Retrieved 25 April 2022 from https://web.archive.org/web/20220131223603/https://sos.ga.gov/index.php/elections/2020_votes_cast_for_certified_write-in_candidates

[22] State of Georgia, *November 3 Presidential Recount Official and Complete Results*, Retrieved 25 April 2022 from https://results.enr.clarityelections.com/GA/107231/web.264614/#/detail/5000

[23] ibid.

[24] Ga. Code Ann. § 21-2-385 (Lexis Advance through the 2021 Regular and Special Sessions of the General Assembly). Retrieved 20 April 2022 from https://advance.lexis.com/api/document/collection/statutes-legislation/id/6348-FW71-DYB7-W2XW-00008-00?cite=O.C.G.A.%20%C2%A7%2021-2-385&context=1000516

[25] U.S. Elections Project, *Georgia Early Voting Statistics*, Retrieved 20 April 2022 from https://electproject.github.io/Early-Vote-2020G/GA.html

[26] Ga. Code Ann. § 21-2-2. Retrieved 20 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-1-general-provisions/section-21-2-2-definitions

[27] ibid.

[28] Ga. Code Ann. § 21-2-285. Retrieved 20 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-8-voting-by-paper-ballot/section-21-2-285-form-of-official-election-ballot-attestation-on-receipt-of-benefit-in-exchange-for-vote-when-an-election-is-not-required

[29] Ga. Code Ann. § 21-2-286-.b(3). Retrieved 20 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-8-voting-by-paper-ballot/section-21-2-286-printing-specifications-numbering-and-binding-of-ballots

[30] Ga. Code Ann. § 21-2-300-.02. Retrieved 20 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-8a-uniform-election-equipment/section-21-2-300-provision-of-new-voting-equipment-by-state-uniform-system-for-all-elections-to-be-conducted-with-use-of-scanning-ballots-marked-by-electronic-ballot-markers-pilot-programs-authorized-county-responsibilities-education-county-and-municipal-contracts-for-equipment

[31] Secure the Vote, *FAQ – How does the new voting system work?*. Retrieved 20 June 2022 from https://securevotega.com/faq/

to "offer each voter specific verbal instruction to review their printed paper ballot prior to scanning it."[32] During an audit or in a case of discrepancy, the plaintext is considered the authoritative component of a ballot: "For ballots marked by electronic ballot markers, the auditors shall rely on the printed text on the ballot to determine the voter's selection."[33]

In the case of a close election, Georgia state law does not require automatic recounts. However, if an election's margin is less than or equal to 0.5%, a candidate can request a machine recount.[34] In the Georgia 2020 General Election, the Georgia Secretary of State ordered a full hand recount of all presidential votes cast.[35]

Georgia uses testing, recount, and auditing procedures to discover discrepancies in marked ballots and ensure proper working election equipment. Several of the relevant procedures are described in Table 4.

Table 4. Summary of Georgia Testing, Recount, and Audit Procedures

Procedure	Description	Summarized Steps[36]	Source
Logic and Accuracy Testing (LAT)	Test performed by all counties at least three days prior to an election. LAT testing ensures proper operation of election equipment (including poll books, BMDs, scanners, and EMS systems) before an election.	• Check poll book ability to accurately look up and check-in voters. • Check BMD touchscreen to ensure the correct display of selections. • Verify paper ballots printed by all BMDs/BMD printers accurately reflect choices selected on BMD touchscreens. • Ensure ballot scanner's ability to accurately scan marked ballots. • Ensure ballot scanner's tabulation on its memory card successfully uploads into EMS. • Ensure tabulations in EMS accurately reflect selections on paper ballots.	SEB Rule 183-1-12-.08 Logic and Accuracy Procedures[37]
Recount	State-level re-tabulation of all ballots through ballot scanners after votes are certified. A recount may be requested by a candidate in a close election (0.5% margin), an election official that suspects an error or discrepancy, or the Georgia Secretary of State. Manual hand recounts may be conducted pursuant to a court order or discrepancies reported during a machine recount.	• Randomly select and manually review at least 100 ballots (75 from electronic BMDs and 25 from hand-marked absentee ballots) across at least 3 precincts. • If no discrepancies are noted during the manual plaintext review, all ballots are tabulated using ballot scanners.	SEB Rule 183-1-15-.03

[32] Ga. Comp. R. & Regs. 183-1-12-.11. Retrieved 20 June 2022 from https://rules.sos.state.ga.us/gac/183-1-12

[33] Ga. Comp. R. & Regs. 183-1-15-.04. Retrieved 20 June 2022 from https://rules.sos.state.ga.us/gac/183-1-15

[34] State of Georgia, *Election Recount Rules in Georgia*, Retrieved 20 April 2022 from https://georgia.gov/election-recount-rules-georgia

[35] Georgia Secretary of State, *2020 General Election Risk-Limiting Audit*. Retrieved 06 June 2022 from https://sos.ga.gov/page/2020-general-election-risk-limiting-audit.

[36] The summarized Georgia testing, recount, and audit procedures provided by MITRE NESL were derived from Georgia rules and laws and do not contain all steps performed or required of election personnel.

[37] Secure the Vote, *January 2020 Logic and Accuracy Procedures v1.0*. Retrieved from J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices*: Exhibit B.

Result Tabulation	After all voting is completed and polls are closed, election officials record and compare the number of voter check-ins and marked ballots before sending the results and materials to a location for official consolidation and tabulation.	• Record count of ballots cast in each scanner. • Print three tapes containing tabulated results from each scanner. Each tape is signed by the election management personnel (if the tapes are believed to be true and correct). • Record count of printed ballots from each BMD printer. • Record count of unsuccessfully scanned ballots in the scanner's emergency bin. • Record count of voter check-ins. • Record count of provisional ballots. • Check to ensure the recorded counts reconcile with each other. • Recorded results, scanner memory cards, and other election equipment are sealed and transported to a location where results are officially consolidated and tabulated. • Upon delivery, the received materials are inspected for tampering and then opened. • Scanner memory card contents are transferred into an EMS and combined with absentee and authorized provisional ballot counts as part of the official consolidation and tabulation process.	SEB Rule 183-1-12-.12
Risk Limiting Audit	Manual post-election audit that involves the review of a statistically significant number of randomly selected ballots to verify the accuracy of reported election outcome.[38] Georgia RLAs are performed by all counties after general elections in even-numbered years and use a maximum risk limit of 10%.	• Election superintendents create 2-person audit boards. • Ballot containers are unsealed, counted, and re-sealed by audit board members. Chain-of-custody is maintained throughout the process. • Audit boards members use only the plaintext portion of ballots marked by electronic BMDs during the counting process. • The audit continues until all selected ballots have been counted and the risk limit is met.	SEB Rule 183-1-15-.04

4 Methodology

To understand the material and make an independent assessment of the researcher's claims, the MITRE NESL team reviewed the July 2021 report and documentation from the Dominion

[38] Lindeman, Mark, and Philip Stark. "A gentle introduction to risk-limiting audits." *IEEE Security & Privacy* 10.5 (2012): 42-49.

Democracy Suite v5.5 Technical Data Package (Appendix A). The team consisted of subject matter experts in election security (including cyber, physical, and human/operating standards and norms), offensive cyber operations, defensive cyber operations, malware analysis, and cyber forensics. The analysis was conducted between 14 March 2022 and 29 April 2022.

To ground the analysis in relevant context, MITRE NESL considered Georgia voting laws, election practices and protocol, and the researcher's report. MITRE NESL performed a technical analysis of the claims in the researcher's report, documenting the information into threat models that incorporate the following information:

- Resources required
- Leveraged vulnerabilities
- Types of attacks
- Obfuscation techniques
- Means, methods, and opportunities of the attacker
- Cyber Kill Chain (based on the MITRE ATT&CK™ Framework)
- Reliability, feasibility, scalability of attack

MITRE NESL used information derived from the threat models to summarize the attacks, their required components, and step-by-step procedures. The proposed attacks were then assessed for feasibility in changing the outcome of an election. Feasibility was determined by qualitatively measuring the following elements:

1. **Difficulty –** General measurement of technical skills needed by personnel to successfully achieve an attack, in whole or in part.
2. **Time-required –** General measurement of time needed to successfully achieve an attack, in whole or in part.
3. **Detectability –** General measurement of the relative ease in which an attack, in whole or in part, evades discovery through physical observation or technical audit.
4. **Scalability –** General measurement of the ability of an attack to affect enough ballots to impact the outcome of an election.

Values for these elements were based on the researcher's proposed attack descriptions and were determined using the criteria listed in Table 5 and the MITRE NESL team's experience supporting cyber operations and election security matters. Scores for detectability and scalability are additionally derived from difficulty and time-required scores. These elements and values were combined into matrices, allowing the MITRE NESL team to assess each attack's overall feasibility in changing the outcome of an election.

Table 5. Criteria Used by MITRE NESL to Assess Feasibility Elements of Proposed Attacks

Measured Element	Value	Criteria
Difficulty	High	Achieving the intended purpose of the attack component requires a highly coordinated team of exceptionally skilled and experienced personnel.
	Moderate	Achieving the intended purpose of the attack component requires some coordination consisting of mid-to-highly skilled and experienced personnel.
	Low	Achieving the intended purpose of the attack component requires minimal coordination involving personnel with entry-level technical skillsets.
Time-Required	High	Achieving the intended purpose of the attack component requires the devotion of a large portion of an attacker's available time considering situational and environmental factors. Assumes an attacker team of exceptionally skilled and experienced personnel.
	Moderate	Achieving the intended purpose of the attack component requires the devotion of a moderate portion of an attacker's available time considering situational and environmental factors. Assumes an attacker team of exceptionally skilled and experienced personnel.
	Low	Achieving the intended purpose of the attack component requires the devotion of a small portion of an attacker's available time considering situational and environmental factors. Assumes an attacker team of exceptionally skilled and experienced personnel.
Detectability	High	The attack is likely discoverable given standard security practices and procedures involving election integrity. Assumes an attacker team of exceptionally skilled and experienced personnel.
	Moderate	The attack has some chance of evading discovery given standard security practices and procedures involving election integrity. Assumes an attacker team of exceptionally skilled and experienced personnel.
	Low	The attack will likely evade discovery given standard security practices and procedures involving election integrity. Assumes an attacker team of exceptionally skilled and experience personnel.
Scalability	High	The attack targets and impacts many voting machines, potentially impacting thousands of ballots, and has a statistically significant chance to impact the outcome of an election.
	Moderate	The attack targets and impacts some voting machines, potentially impacting hundreds of ballots, and is not likely to impact the outcome of an election.
	Low	The attack targets and impacts a single voting machine, impacting a statistically insignificant number of votes, and will not impact the outcome of an election.

As MITRE NESL did not have access to Georgia voting equipment or the researcher's proof-of-concept capabilities, the researcher's reported technical implementations were assumed to be valid and working.

A list of compensating controls assumed by MITRE NESL when conducting its technical analysis (Section 5) and assessment of claims (Section 6) can be found in Appendix B.

5 Technical Analysis

The researcher proposed multiple proof-of-concept attacks against Dominion Democracy Suite 5.5-A utilizing both hardware and software. The MITRE NESL team analyzed the researcher's

reported vulnerabilities and exploitation methods and assessed their feasibility in changing the outcome of a Georgia election. Where necessary, MITRE NESL attempted to fill in gaps of information omitted from the researcher's stated approach. These assumptions are noted appropriately.

Analysis of the supporting components for the researcher's proposed attacks is provided in Section 5.1. Section 5.2 provides an assessment of how these components are collectively used in the proposed attack scenarios.

5.1 Supporting Components for Proposed Attacks

The MITRE NESL team reviewed and assessed the supporting components utilized by the researcher in the proposed attacks. These components included QR code content interpretation, Raspberry Pi devices, a forged technician card, a poll worker card, an infinite voter card, modified ICX application files, an automated keystroke scripting device, a modified Election Definition File (EDF), and log manipulation. Each of the components are summarized and linked to attacks proposed by the researcher.

5.1.1 Quick Response Code Content Interpretation

A QR code is a two-dimensional barcode used to conveniently store and convey information to devices that can decode its contents. Georgia's BMD systems use QR codes to store a voter's ballot selections during an election. QR codes appear on printed paper ballots along with a plaintext summary of the voter's candidate selections. When a voter inserts a printed ballot into a scanner, the scanner captures, decodes, and validates the data encoded in the QR code before recording the ballot selections.

The researcher stated that data stored in a ballot's QR code is written in byte mode[39] in an unencrypted format understood by Dominion systems. The encoded data structure includes metadata for the ballot, the ballot selections, and the computed message authentication code (MAC)[40] based on the ballot selections. Ballot selections are encoded as 0 or 1 in the QR code data structure, and these selections correspond to the candidates listed in the voter's ballot style.

The researcher asserts that they decoded a ballot's QR code using freely available software named Scandit Barcode Scanner for iOS[41] and Zbar.[42] The decoded content was mentioned to have been further reverse engineered and tested using Dominion's ImageCast Remote Accessible Vote-By-Mail web-based software.

The researcher also asserts that the computed MAC in a QR code is based only on a voter's ballot selections and is not unique to a ballot. The notion was reportedly validated by performing a replay attack (i.e., inserting multiple copies of the same ballot into a scanner) in a laboratory setting.

[39] In a QR code, byte mode refers to a generic method that allows QR code producers to represent approximately 3 KB of data.

[40] MACs are cryptographically computed values used to protect a ballot's data integrity. More information about MACs can be found here: https://csrc.nist.gov/csrc/media/publications/fips/198/1/final/documents/fips-198-1_final.pdf.

[41] Scandit AG. *Scandit Barcode Scanner*. Apple App Store, https://apps.apple.com/us/app/scandit-barcode-scanner/id453880584.

[42] ZBar. ZBar Bar Code Reader. GitHub, https://github.com/mchehab/zbar.

MITRE NESL assesses that QR code content interpretation requires knowledge of Dominion's encoding format, knowledge of ballot styles (since ballots vary by districts/counties), access to a ballot QR code, and access to a QR code scanner that can parse byte mode content.

The researcher references the use of QR code interpretation in the proposed BMD Printer Attack (Section 5.2.1).

5.1.2 Raspberry Pi Devices

Raspberry Pi devices are small computers that can be programmed to efficiently perform any number of tasks. They support most modern-day programming languages and execution environments. Raspberry Pi devices are low cost and come in several sizes. The researcher mentions using Raspberry Pi Zero W devices, which are 65mm x 30mm—roughly half the size of a credit card. The model features one USB port.

The researcher asserts that they programmed two Raspberry Pi devices to fraudulently alter ballot print jobs in a laboratory setting. The devices were allegedly instructed to intercept and selectively modify print jobs received by a printer. The researcher did not specify which printer drivers were utilized in the malicious hardware.

MITRE NESL assesses that programming Raspberry Pi devices to modify print jobs requires detailed knowledge of the received content (i.e., an ability to decode QR codes), access to a target printer model, and access to Raspberry Pi devices.

The researcher references the use of Raspberry Pi devices in the proposed BMD Printer Attack (Section 5.2.1). The researcher also discusses a potential use of a Raspberry Pi device in the Infinite Voter Card / Photocopied Ballot Attack (Section 5.2.6).

5.1.3 Forged Technician Card

Technician cards are smart cards with an integrated circuit that, when combined with a PIN, allow technicians to perform system administration functions on BMDs. Technician tasks include copying election definition files onto BMDs, performing system configurations, installing software updates, and exporting election applications and logs.

After reportedly analyzing the security of a technician card in a laboratory setting, the researcher asserts that Dominion's system communications use International Organization for Standardization (ISO) 7816-4[43] to check aspects of files found on a technician card. The researcher also claims that the card enables technicians to exit the ICX application and take advantage of elevated access privileges available on the Android operating system.

The researcher asserts that they created an unofficial ("forged") technician card by purchasing and modifying a programmable smart card called a Java Card. The Java Card was reportedly modified to accept any PIN from a BMD and acknowledge any requested file as present. The Java card was also programmed to transmit empty files when requested by the ICX application during the authentication process. These steps were allegedly sufficient to grant technician-level access to users of the forged technician card.

[43] More information about the ISO 7816-4 protocol can be found here: https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-4:ed-4:v1:en.

MITRE NESL assesses that creating a forged technician card requires knowledge of Dominion system communication protocol, access to a smart card reader/writer, and access to a programmable smart card.

The researcher references the use of a forged technician card in the proposed Technician Card Attack (Section 5.2.2).

5.1.4 Poll Worker Card

Poll worker cards are smart cards with an integrated circuit that, when combined with a PIN, allow poll workers to perform administrative election tasks involving BMDs. Poll worker tasks include starting and stopping voting periods, checking machine counters, printing polling related data, and activating manual ballot sessions on BMDs.

After reportedly analyzing the security of a poll worker card in a laboratory setting, the researcher asserts that Dominion's system communications use ISO 7816-4 to check aspects of files found on the card. Further, the researcher claims to having found cryptographic secrets on poll worker cards that were re-used in other parts of the election system. For example, the same encryption keys found on the poll worker card are reportedly also used to decrypt election definition files, generate MAC values in QR codes, and decrypt election results from scanner memory cards. The researcher noted that these secrets are shared at the county level in Georgia and can be reused across many precincts in the same county.

The researcher asserts they created a custom software capability that extracts cryptographic secrets from a poll worker card inserted into a commercial smart card reader. The secrets are allegedly copied when a user enters the card's PIN into the software capability.

MITRE NESL assesses that creating a data extraction capability from a poll worker card requires knowledge of Dominion system communication protocol, access to an official poll worker card, the card's PIN, and a smart card reader. While not specifically described by the researcher, MITRE NESL also assesses it would be necessary to use a software/hardware monitoring tool to intercept, record, study, and understand the system communications between a BMD and a poll worker card to develop the capability.

The researcher references the extraction of cryptographic secrets in the proposed EMS Attack (Section 5.2.5).

5.1.5 "Infinite" Voter Card

Voter cards are distributed to voters upon check-in at a polling location and subsequently used to activate voting sessions when inserted into BMDs. Voter cards are automatically deactivated after a voter selects to print their ballot. A card is returned to a poll worker after each ballot is scanned. An infinite voter card is an unofficial voter card that does not deactivate after a ballot is printed, theoretically allowing a voter to print multiple ballots.

The researcher asserts they created an unofficial voter card despite not being provided with a voter card as part of the equipment received for the assessment. The researcher's report did not specifically state how knowledge was obtained to create the card (other than through "reverse engineering"[44]). The researcher noted that Dominion's system communications use ISO 7816-4 to check aspects of files found on a voter card. It is also mentioned that when a person inserts a

[44] J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices.* p. 31.

voter card into a BMD, the BMD's ICX application reportedly sends a hard-coded PIN to the card to access its contents and validates its authenticity through an Election Signature on the card. After a successful validation, a voter fills out their ballot on the BMD.

The researcher reportedly created an infinite voter card using a purchased programmable smart card and tested it in a laboratory setting by printing multiple ballots without the card being deactivated by the ICX/BMD. The researcher reportedly intercepted the hard-coded PIN sent from the ICX application, extracted an Election Signature,[45] and stored them both on the programmable smart card.

MITRE NESL assesses that creating an infinite voter card requires knowledge of Dominion's system communication protocol, physical access to a BMD, access to a programmable smart card, access to a smart card reader/writer, and knowledge of the hard-coded PIN and Election Signature (which may also require access to a voter card or a poll worker card and PIN).

An infinite voter card is used as part of the proposed Infinite Voter Card / Photocopied Ballot Attack (Section 5.2.6).

5.1.6 Modified ImageCast X Application

Dominion's ICX software is bundled by Dominion into a standard Android application installation file format called an Android Package (APK). APKs are distributed and installed on Georgia BMDs, which run the Android operating system.

The researcher reportedly extracted the ICX software,[46] reverse engineered it, and modified it to fraudulently alter ballot selections in a laboratory setting using the following process:

1. **Obtain a copy of the original application.** The researcher allegedly obtained a copy of the ICX application by physically accessing a BMD in a laboratory setting and extracting the application's APK file. The researcher suggested two methods attackers can potentially use to obtain this file: 1) physically access a BMD with a forged technician card as part of a Technician Card Attack (Section 5.2.2); or 2) obtain a USB drive distributed to election officials that is used to perform software updates on BMDs.
2. **Reverse engineer the original application.** The researcher asserts they reverse engineered the ICX application by disassembling the APK and identifying places in the code to insert malicious functionality.
3. **Insert new (malicious) functionality.** The researcher reportedly wrote a malicious ballot-manipulating software library and inserted it into the ICX software. While not specifically stated by the researcher, MITRE NESL assesses that this step requires previous knowledge of a name, party, or other identifier if an attacker is aiming to achieve a particular electoral outcome.
4. **Package software into a new application.** The researcher reportedly bundled the modified software code into an APK file using a similar process Dominion used to create the original file.

[45] The researcher's report did not indicate how the Election Signature was obtained. MITRE NESL assumed the content was extracted from an official poll worker card and PIN (as described in Section 5.1.4). The researcher also discussed a scenario where an Election Signature could be extracted using an official voter card, two programmable smart cards, a Raspberry Pi device, and a smart card reader.

[46] The researcher notes they had access to ICX software versions 5.5.10.30 and 5.5.10.32.

5. **Test the modified application on a BMD.** While not specifically stated by the researcher, MITRE NESL assumed the researcher tested the modified ICX software on a BMD system to validate that the modifications worked as expected. The researcher alludes to testing in a note that mentions, "These demonstrations have minor imperfections (such as delays or small visual glitches)."[47]

The researcher noted several anti-detection techniques that could be integrated into the modified ICX software. These additional modifications would be included as new functionality (Step 3 above). The following technical and procedural controls were addressed by the researcher.

- **Display of Application Hash.** The ICX application displays a hash of the installed ICX application (APK file) on-screen, a feature which has been used in field audits to verify application integrity.[48] A malicious version of the ICX application was reportedly programmed by the researcher to display the expected hash of the original ICX application.
- **Application Export.** The technician mode of the ICX application includes a software feature to export the application's APK file to a USB drive, which can be forensically analyzed on a trusted computer. This ICX application feature has also been used in field audits to verify application integrity.[49] A malicious version of the ICX application was reportedly programmed by the researcher to subvert this check and instead export a copy of the original APK when a technician presses the "Export Apps" button.
- **MAC Authentication.** MACs are cryptographically computed values that help ensure the integrity of data encoded in a ballot's QR code. It was asserted that the researcher's malicious ICX application was programmed to perform all ballot-manipulating code instructions before MAC calculations occur in the software, allowing the MAC calculations to happen normally. This design factor reportedly alleviates the need to obtain an encryption key. Alternatively, the researcher suggests that the secret key used in MAC calculations can be extracted from the ICX software and used to create valid MACs.
- **Logic and Accuracy Testing (LAT).** LAT testing ensures proper operation of election equipment and is performed by counties at least three days prior to an election.[50] The researcher suggests that LAT testing could be detected and subverted by malicious ICX software that monitors the date/time, the number of printed ballots, the rate of voting, the pattern of votes, the number of corrected mistakes, or use other factors that might distinguish a real voting session from a LAT testing session.

The researcher reportedly used two methods to install a modified ICX application onto a Georgia BMD: side loading, and "ahead-of-time" (OAT) file replacement. For brevity, OAT files are further referred to as "OATs."

---

[47] J. Alex Halderman, *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, 1 July 2021. p. 19

[48] ibid., Exhibit C (p. 5)

[49] ibid., Exhibit C (p. 5)

[50] Ga. Comp. R. & Regs.183-1-12-.08. Retrieved 05 Jun 2022 from https://casetext.com/regulation/georgia-administrative-code/department-183-rules-of-state-election-board/chapter-183-1-georgia-election-code/subject-183-1-12-preparation-for-and-conduct-of-primaries-and-elections/rule-183-1-12-08-logic-and-accuracy-testing.

- **Side Loading.** BMDs allow the installation of Android applications from unknown sources in the Android Settings menu. By enabling this feature, a user can install an APK file from a USB drive through several methods. The side loading installation process used by the researcher involves tapping an application of interest in the File Manager application, which is available by default on most Android systems.

  The researcher references side loading in several of the local proof-of-concept attacks.

- **OAT Replacement**. The Android operating system includes an application performance feature, which uses an application's optimized code file (an OAT) to speed up the launch time and improve an application's general responsiveness. An OAT is generated for each application upon install and re-generated each time the application is updated. The researcher allegedly used a technique demonstrated at the Black Hat® Asia 2015 conference to replace an application's OAT with a malicious version.[51] The technique depends on the ability to insert metadata from the original application's OAT into the newly modified application's OAT. The new OAT can then be copied to a BMD and replace the original ICX application's OAT. This action requires elevated privileges on the BMD, which were reportedly available on the equipment the researcher assessed.

  This method is referenced by the researcher in the proposed EMS Attack (Section 5.2.5).

MITRE NESL assesses that modifying the ICX application requires physical access to a BMD, access to the version of ICX application used in a target election, and access to reverse engineering software.

Modified ICX applications are used or referenced in the proposed Technician Card Attack (Section 5.2.2), Bash Bunny Attack (Section 5.2.3), Safe Mode Attack (Section 5.2.4), and EMS Attack (Section 5.2.5).

5.1.7 Automated Keystroke Scripting Device

An automated keystroke scripting device is programmable hardware that acts as an all-in-one USB keyboard and storage drive. When the hardware is attached to a machine via a USB cable, the keystroke scripting device powers on and attempts to execute a set of pre-programmed actions. These actions can include keyboard keystrokes, file transfers, and button presses at designated pixel coordinates.

The researcher asserts they used a Bash Bunny (one of various automated keystroke scripting products available on the market) in a laboratory setting to automate keystrokes, button presses, and file copies on a BMD.

MITRE NESL assesses that the use of automated keyboard scripting devices in proposed attack scenarios requires physical access to a BMD, access to an automated keyboard scripting device, and knowledge of available Android system commands, Android menus and buttons, and on-screen pixel coordinates.

Automated keyboard scripting devices are referenced in the proposed Bash Bunny Attack (Section 5.2.3) and the Technician Card Attack (Section 5.2.2).

[51] P. Sabanal, *Hiding Behind ART*, Black Hat Asia 2015, https://www.blackhat.com/docs/asia-15/materials/asia-15-Sabanal-Hiding-Behind-ART-wp.pdf

5.1.8 Modified Election Definition File

Election Definition Files (EDFs) are created within Election Management Systems (EMSs) and contain ballot style definitions specific to a county and its districts. They are placed on USB sticks and are managed by election officials at a central location. The USB sticks are inserted into BMDs and the EDFs are installed through the ICX application prior to pre-election logic and accuracy testing by election officials. EDFs are encrypted zip files, referred to in the researcher's report as "ICX.dat."

The researcher asserts that the EDF encryption key[52] for an ICX.dat file can be obtained from an EMS, an Election Project database,[53] or from a Poll Worker Card with knowledge of its PIN (Section 5.1.4).

The researcher also asserts that EDFs are not digitally signed. This allegedly allowed the researcher to decrypt the EDF (using the derived encryption key), insert ballot-manipulating software into the EDF, and re-encrypt the file with the original encryption key without failing integrity checks on a tested BMD in a laboratory setting.

MITRE NESL assesses that the use of modified EDFs requires access to an EDF file, an EDF file encryption key, a modified ICX application (Section 5.1.7), and physical access to a BMD.

These modified EDFs are used as part of the proposed EMS Attack (Section 5.2.5).

5.1.9 Log Manipulation

Logs are files that contain records of application usage data and events. These records can be reviewed for troubleshooting or auditing purposes.

The researcher asserts to having identified several types of logged information which attackers can modify to cover their tracks. These included a "public counter" of ballots printed during the current contest, a "lifetime counter" of ballots printed by the machine since its creation, and timestamped records of administrative accesses, openings/closings of polling sessions, and removable media attachment/detachment events.

The researcher notes that access to ICX log files is only controlled by filesystem permissions and no log file integrity checks are conducted by the system. The researcher reportedly performed a test in a laboratory setting where modifications were made to a BMD's lifetime counter and access log through use of the BMD's pre-installed applications. The Safe Mode Attack (Section 5.2.4) was referenced as an example method of how an attacker could potentially gain privileges needed to bypass permission controls and modify existing logs. The researcher also theorized a scenario where log manipulation could be automated in a similar manner to how the proposed EMS Attack (Section 5.2.5) distributes modified EDFs (Section 5.1.8).

MITRE NESL assesses that the manipulation of BMD audit log files requires physical access to a BMD, elevated access privileges, a mechanism to navigate to and open BMD operating system files, and knowledge of relevant ICX auditing information and log file locations.

[52] For the purposes of this report, "encryption key" refers to the initialization vector (IV) and symmetric encryption key used to encrypt or decrypt election materials.

[53] An Election Project database is a structured set of election data used by an EMS and EMS users to configure and create EDFs. An Election Project database can be imported into an EMS through an "Election Package," a transferrable zip file.

The researcher did not assert that they implemented log manipulation into any proposed attack scenario but noted that real attacks could take advantage of the privilege escalation opportunity on BMDs to modify audit log files.

5.2 Proposed Attack Scenarios

MITRE NESL identified six distinct proposed attack scenarios hypothesized by the researcher that have a potential to change voter ballots. Attack scenarios, as defined by MITRE NESL, are combinations of steps performed by an attacker (or a team of attackers) to bypass compensating controls, affect election equipment, and influence an election outcome. In the July 2021 report, the researcher assessed and reportedly developed attack capabilities against a broad array of Dominion equipment and components. MITRE NESL chose to focus on the proposed attack scenarios that have the potential to change ballots. Other attacks in the researcher's principal findings or main conclusions are addressed in Section 6.

Each of the six attack scenarios comprise one or more supporting components (listed in Section 5.1). The proposed attack scenarios have been renamed for clarity and are presented in the same order as they appear in the July 2021 report. The attack scenarios include:

1. **BMD Printer Attack -** BMD printer hardware tampering using Raspberry Pi devices.
2. **Technician Card Attack -** Install local malware using forged technician card.
3. **Bash Bunny Attack -** Install local malware using automated keystroke scripting device.
4. **Safe Mode Attack -** Install local malware using alternate Android mode.
5. **EMS Attack** - Distribute malware using modified EDF files.
6. **Photocopied Ballot Attack* -** Ballot stuffing using photocopier or infinite voter cards.

**The Photocopied Ballot Attack comprises two attacks mentioned by the researcher. MITRE NESL combined them for clarity due to their similarity.*

The goal of these proposed attacks, as the researcher mentioned, was to "alter voters' votes while subverting all of the procedural protections practiced by the State."[54] The researcher claimed, "Many of the attacks I successfully implemented could be effectuated by malicious actors with very limited time and access to the machines, as little as mere minutes"[55] and that "ICX malware can still change individual votes and most election outcomes without detection."[56]

Alternatively, should the attack fail to produce the intended electoral decision, an adversary aiming to reduce confidence in the election could use the knowledge that ballots had been modified (and counted as modified) to question the legitimacy of the electoral results. The researcher acknowledges this secondary objective while summarizing the report's main conclusions: "Georgia's BMDs are so vulnerable [it] is all but certain to be exploited by partisan actors to suppress voter participation and cast doubt on the legitimacy of election results."[57]

[54] J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices.* p. 4.

[55] ibid., p. 4.

[56] ibid., p. 6.

[57] ibid., p. 8.

5.2.1 Ballot Marking Device Printer Attack

In a proof-of-concept attack proposed by the researcher, two malicious Raspberry Pi devices were reportedly attached and hidden inside a BMD printer (HP LaserJet M402dne) and connected to the printer's power supply. The devices allegedly capture a ballot, modify the ballot's embedded QR code selections[58] in favor of the preferred candidate, and then print the modified ballot.

According to the researcher's proposed attack description, the malicious hardware replaces the physical USB cord inside the printer with one of the devices capturing and sending ballots wirelessly to the other for ballot interpretation and modification. If a ballot selection is not in favor of the preferred candidate, the software is described to replace the QR code with a randomly selected QR code from a set of previously encountered favorable ballots while keeping the plaintext of the original ballot intact. When the ballot is printed, the plaintext reflects the voter's original selections.

To perform this attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Detect and decode a QR code in the raw data transmission sent to a printer
- Interpret QR code content (Section 5.1.1)
    - Possess knowledge of Dominion's encoding format
    - Possess knowledge of election related information (e.g., precinct, ballot styles) specific to an ICX BMD
    - Obtain access to a ballot QR code
    - Obtain access to a QR code scanner that can parse byte mode content
- Configure Raspberry Pi (or equivalent) hardware (Section 5.1.2)
    - Possess ability to interpret QR codes
    - Obtain access to target printer model (available through public procurement documents)
    - Obtain access to Raspberry Pi devices
- Obtain access and possess ability to disassemble and reassemble printer hardware components

5.2.1.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and Georgia risk-limiting audits to determine that the BMD Printer Attack is non-scalable, detectable, and requires a high degree of access. Table 6 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and

[58] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

definitions stated in Section 4. The values in Table 6 also assumed that the proposed attack would be performed against a single device (otherwise attacking multiple devices will increase "Time Required" and decrease "Overall Feasibility").

Table 6. BMD Printer Attack Feasibility Matrix

Attack Component	**Details**	**Difficulty**	**Time Required**	**Overall Feasibility**
QR Code Content Interpretation	Create software that decodes and interprets content from a submitted ballot in a target election	Moderate	High	Moderate
Configurating Raspberry Pi Devices	Create software that modifies a ballot	Moderate	Moderate	Moderate
	Integrate software into Raspberry Pi hardware devices	Low	Low	High
Inserting Raspberry Pi Devices into BMD Printer	**Access/obtain BMD Printer that will be used in a target election**	**High**	**Moderate**	**Low**
	Access/obtain a printer of the same make/model as BMD Printer for testing	Low	Low	High
	Install the hardware devices into the printer (i.e., remove casing, unplug/plug-in hardware)	Moderate	High	Moderate
Detectability	**Attack avoids detection by poll workers, other voters (e.g., poll worker detects someone tampering with equipment at a polling station) at precinct**	**High**	**High**	**Low**
	Attack avoids detection by staff (e.g., security detects someone tampering with equipment in a warehouse) at county storage location	**High**	**High**	**Low**
	Attack avoids detection through an RLA	**High**	**Low***	**Low**
	Attack avoids detection through result tabulation[59]	Low	Low*	High
Scalability	**Attack can be performed on many BMDs**	**High**	**High**	**Low**

** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the researcher's proposed BMD Printer Attack's feasibility are access, detectability, and scalability.

- **Limited Access to BMD Printers.** This proposed attack relies on access to BMD printers used in Georgia elections. Obtaining access to the printers before an election may be difficult without the help of an insider or intruder.
- **High Detectability.** The proposed BMD Printer Attack would most likely occur at a county storage or polling location since some knowledge of ballot styles is required. Assuming the attack occurs in one of these locations, an attacker would need to bypass

[59] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

physical and operational security controls. The proposed BMD Printer Attack is also detectable through an RLA.

- **Limited Scalability.** Since the proposed BMD Printer Attack targets one BMD Printer at a time, the number of potentially affected votes in a Georgia election would be statistically insignificant[60] to change the outcome of an election and avoid a recount.

5.2.2 Technician Card Attack

In a proof-of-concept attack proposed by the researcher, a forged technician card was reportedly used to gain privileged access to a Georgia BMD to install ballot manipulating malware in a laboratory setting. The forged technician card reportedly contains a file identifying it as an administrative card with the Technician record value set (distinguishing it from a poll worker card). The attacker allegedly used this privileged access to install a modified ICX application on the BMD.

The researcher describes the modified ICX software as having been programmed to change voters' ballot selections embedded in the printed QR codes[61] in favor of the preferred candidate. The researcher asserts that the modified ballots are accepted by an ICP Scanner. The researcher also mentions that the modified ICX software installation process can be aided by an automated keystroke scripting device. After completing the software installation process and removing the technician card from the BMD, the researcher asserts the modified ICX software remains running on the BMD after the attacker leaves.

To perform this attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Modify the ICX application software (Section 5.1.6)
    - Obtain physical access to BMD
    - Obtain access to specific version of ICX application used in a target election
    - Obtain access and ability to use reverse engineering software
- Create a forged technician card (Section 5.1.3)
    - Possess knowledge of Dominion system communication protocol
    - Obtain access to smart card reader/writer
    - Obtain access to programmable smart card
- Obtain physical access to BMD USB port
- Possess knowledge of election related information (e.g., precinct, ballot style) specific to the ICX BMD

[60] Assuming each BMD prints 225 ballots, attacking a single BMD would not have a statistically significant chance at changing the outcome of an election and avoiding a recount. In practice, MITRE NESL also assumes that this attack would be implemented in such a way to only affect a fraction of unfavorable votes to avoid detection during vote tabulation and auditing. This further increases the number of BMD printers requiring an attack to change the outcome of an election.

[61] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

5.2.2.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and Georgia risk-limiting audits to determine that the proposed Technician Card Attack is non-scalable, detectable, and requires a high degree of access. Table 7 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and definitions stated in Section 4. The values in Table 7 also assumed that the proposed attack would be performed against a single device (otherwise attacking multiple devices will increase "Time Required" and decrease "Overall Feasibility"). MITRE NESL additionally assumed the use of some automation to install the modified ICX application.

Table 7. Technician Card Attack Feasibility Matrix

Attack Component	Details	Difficulty	Time Required	Overall Feasibility
Forged Technician Card	Access/obtain knowledge about the authentication protocol used between BMDs and Technician Cards	Moderate	Moderate	Moderate
	Access/obtain real Technician Card and PIN for testing and protocol discovery	High	Moderate	Low
	Access/obtain BMD hardware and software for testing and protocol discovery	High	Moderate	Low
	Create forged technician card, assuming knowledge of authentication protocol	Low	Low	High
Modified ICX Application	**Access/obtain ICX software application used in a target election**	**High**	**Moderate**	**Low**
	Reverse-engineer ICX software application	Moderate	Moderate	Moderate
	Insert malicious functionality into application	High	Low	Moderate
	Repackage Application	Low	Low	High
	Access/obtain BMD hardware and software equipment for testing	**High**	**Moderate**	**Low**
Automate / Scripting Actions on BMD *(optional)*	**Access/obtain BMD hardware and software equipment for testing**	**High**	**Moderate**	**Low**
	Configure software to perform file transfers, keystrokes, and button presses (through pixel coordinates)	Moderate	Moderate	Moderate
Detectability	Attack avoids detection by poll workers, other voters (e.g., poll worker detects someone inserting a card and installing malware at a polling station) at precinct while polls are open	High	Low	Moderate*
	Attack avoids detection by election officials (e.g., security detects someone inserting a card and installing malware at a warehouse) at county storage location	Moderate	Low	Moderate
	Attack avoids detection through an RLA	**High**	**Low****	**Low**

	Attack avoids detection through result tabulation[62]	Low	Low**	High
Scalability	**The attack can be performed on many BMDs**	**High**	**High**	**Low**

** A poll worker card (Section 5.1.4) may be required to continue polling upon the launch of the ICX application on a BMD.[63] This step was not mentioned in the researcher's report. If required, the need for a poll worker card would increase the detectability of the Technician Card Attack and force an attacker to 1) obtain a working poll worker card and PIN, or 2) further manipulate the malicious software to bypass the card/PIN requirement.*

*** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the proposed Technician Card Attack's feasibility are access, time, detectability, and scalability.

- **Limited Access to ICX Application.** This proposed attack relies on access to the specific ICX software version running on Georgia BMDs for a target election. Obtaining this software may be difficult without the help of an insider or intruder.
- **Limited Time Window.** This proposed attack requires time to modify and then install the ICX application. The amount of time (and hence the number of possible modified ballots) decreases as the attack is deployed over the course of an election.
- **High Detectability.** The proposed Technician Card Attack is detectable through an RLA.
- **Limited Scalability.** Since the proposed Technician Card Attack targets one BMD at a time, the number of potentially affected votes in a Georgia election would be statistically insignificant[64] to change the outcome of an election and avoid a recount.

5.2.3 Bash Bunny Attack

In a proof-of-concept attack proposed by the researcher, an automated keystroke scripting device in the form of a Bash Bunny was reportedly used to install a modified ICX application on a Georgia BMD in a laboratory setting. The researcher describes the hardware as an all-in-one USB keyboard and storage device that automatically triggers a series of pre-programmed modifications to the BMD when plugged in via a USB cable.

The asserted modifications, made by the Bash Bunny, include changes to the Android system settings, file copies, and the installation of the researcher's modified ICX software, which was allegedly programmed to change voters' ballot selections in the printed ballot's QR code.[65] After completing the software installation process and removing the Bash Bunny hardware from the

[62] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

[63] Dominion Voting Systems Corp. *Democracy Suite ImageCast X User Guide*, Aug 2018. p. 49

[64] Assuming each BMD prints 225 ballots, attacking a single BMD would not have a statistically significant chance at changing the outcome of an election and avoiding a recount. In practice, MITRE NESL also assumes that this attack would be implemented in such a way to only affect a fraction of unfavorable votes to avoid detection during vote tabulation and auditing. This further increases the number of BMDs requiring an attack to change the outcome of an election.

[65] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

BMD, the researcher mentions that the modified ICX software remains running on the BMD after the attacker leaves.

The Bash Bunny attack, as described by the researcher, takes advantage of apps left running in the background during an ICX software update in October 2020. The background apps can be accessed through an Alt-Tab key combination and provide a means for an attacker to install a malicious ICX application.

To perform this attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Modify the ICX application software (Section 5.1.6)
    - Obtain physical access to BMD
    - Obtain access to specific version of ICX application used in a target election
    - Obtain access and ability to use reverse engineering software
- Pre-program an automated keystroke scripting device (Section 5.1.7)
    - Obtain physical access to BMD
    - Obtain access to automated keystroke scripting device
    - Possess knowledge of Android system commands, menus/buttons, on-screen pixel coordinates
- Obtain physical access to USB port
- Operate in a manner at a polling station to avoid detection
- Possess knowledge of election related information (e.g., precinct, ballot style) specific to the ICX BMD

5.2.3.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and Georgia risk-limiting audits to determine that the proposed Bash Bunny Attack is non-scalable, detectable, and requires a high degree of access. Table 8 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and definitions stated in Section 4. The values in Table 8 also assumed that the proposed attack would be performed against a single device (otherwise attacking multiple devices will increase "Time Required" and decrease "Overall Feasibility").

Table 8. Bash Bunny Attack Feasibility Matrix

Attack Component	Details	Difficulty	Time Required	Overall Feasibility
Modified ICX Application	**Access/obtain ICX software application used in a target election**	**High**	**Moderate**	**Low**
	Reverse-engineer ICX software application	Moderate	Moderate	Moderate
	Insert malicious functionality into application	High	Low	Moderate
	Repackage Application	Low	Low	High
	Access/obtain BMD hardware and software equipment for testing	**High**	**Moderate**	**Low**
Automate/Scripting Actions on BMD	**Access/obtain BMD hardware and software equipment for testing**	**High**	**Moderate**	**Low**
	Configure software to perform file transfers, keystrokes, and button presses (through pixel coordinates)	Moderate	Moderate	Moderate
Detectability	Attack avoids detection by poll workers, other voters (e.g., poll worker detects someone inserting a Bash Bunny at a polling station)	High	Low	Moderate*
	Attack avoids detection by poll workers, other voters while polls are open (e.g., voters notice abnormalities on equipment or ballot)	Low	Low	High
	Attack avoids detection through an RLA	**High**	**Low****	**Low**
	Attack avoids detection through result tabulation[66]	Low	Low**	High
Scalability	**The attack can be performed on many BMDs**	**High**	**High**	**Low**

** A poll worker card (Section 5.1.4) may be required to continue polling upon the launch of the ICX application on a BMD.[67] This step was not mentioned in the researcher's report. If required, the need for a poll worker card would increase the detectability of the Bash Bunny Attack and force an attacker to 1) obtain a working poll worker card and PIN, or 2) further manipulate the malicious software to bypass the card/PIN requirement.*

*** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the Bash Bunny Attack's feasibility are access, time, detectability, and scalability.

- **Limited Access to ICX Application.** This proposed attack relies on access to the specific ICX software version running on Georgia BMDs for a target election. Obtaining this software may be difficult without the help of an insider or intruder.

[66] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

[67] Dominion Voting Systems Corp. *Democracy Suite ImageCast X User Guide*, Aug 2018. p. 49

- **Limited Access to Voting Equipment.** Testing the Bash Bunny Attack requires BMD equipment, which may be difficult without the help of an insider or intruder.
- **Limited Time Window.** This proposed attack requires time to modify and then install the ICX application. The amount of time (and hence the number of possible modified ballots) decreases as the attack is deployed over the course of an election.
- **High Detectability.** The proposed Bash Bunny Attack is detectable through an RLA.
- **Limited Scalability.** Since the proposed Bash Bunny Attack targets one BMD at a time, the number of potentially affected votes in a Georgia election would be statistically insignificant[68] to change the outcome of an election and avoid a recount.

5.2.4 Safe Mode Attack

In a proof-of-concept attack proposed by the researcher, a BMD was reportedly rebooted into an alternate Android mode known as "safe mode" that provides access and privileges needed to install software. Safe mode was allegedly entered by pressing and holding the power button, which then prompted a user to "reboot to safe mode." Although the researcher describes the BMD's door to the power button as tamper-sealed, they note that there were openings in the door that a thin metal tool could be inserted into to achieve a button press.

The July 2021 report states safe mode as an access vector for attackers to install "vote-stealing malware"[69] on a BMD but does not clearly articulate whether the researcher installed or tested any ballot manipulating software through safe mode during their assessment. MITRE NESL assumes the researcher intended to convey the idea that this access method could be used to install and run a modified ICX application in a similar fashion as described in the other attack scenarios (Technician Card Attack and Bash Bunny Attack) to change voters' ballot selections in printed QR codes.[70]

To perform this attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Modify the ICX application software (Section 5.1.6)
    - Obtain physical access to BMD
    - Obtain access to specific version of ICX application used in a target election
    - Obtain access and ability to use reverse engineering software
- Obtain physical access to BMD power button
- Obtain physical access to USB port
- Possess knowledge of election related information (e.g., precinct, ballot style) specific to the ICX BMD

[68] Assuming each BMD prints 225 ballots, attacking a single BMD would not have a statistically significant chance at changing the outcome of an election and avoiding a recount. In practice, MITRE NESL also assumes that this attack would be implemented in such a way to only affect a fraction of unfavorable votes to avoid detection during vote tabulation and auditing. This further increases the number of BMDs requiring an attack to change the outcome of an election.

[69] J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices.* p. 39.

[70] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

5.2.4.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and Georgia risk-limiting audits to determine that the Safe Mode Attack is non-scalable, detectable, and requires a high degree of access. Table 9 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and definitions stated in Section 4. The values in Table 9 also assumed that the proposed attack would be performed against a single device (otherwise attacking multiple devices will increase "Time Required" and decrease "Overall Feasibility"). MITRE NESL additionally assumed the use of some automation to install the modified ICX application.

Table 9. Safe Mode Attack Feasibility Matrix

Attack Component	Details	Difficulty	Time Required	Overall Feasibility
Modified ICX Application	**Access/obtain ICX software application used in a target election**	**High**	**High**	**Low**
	Reverse-engineer ICX software application	Moderate	Moderate	Moderate
	Insert malicious functionality into application	High	Low	Moderate
	Repackage Application	Low	Low	High
	Access/obtain BMD hardware and software equipment for testing	**High**	**Moderate**	**Low**
Automate / Scripting Actions on BMD *(optional)*	**Access/obtain BMD hardware and software for automation testing**	**High**	**Moderate**	**Low**
	Configure software to perform file transfers, keystrokes, and button presses (through pixel coordinates)	Low	Low	High
Detectability	**Attack avoids detection by poll workers, other voters (e.g., poll worker detects someone rebooting a BMD and installing malware at a polling station) at precinct**	**High**	**Moderate**	**Low***
	Attack avoids detection by election officials (e.g., security detects someone rebooting a BMD and installing malware at a warehouse) at county storage location	High	Moderate	Low
	Attack avoids detection through an RLA	**High**	**Low****	**Low**
	Attack avoids detection through result tabulation[71]	Low	Low**	High
Scalability	**The attack can be performed on many BMDs**	**High**	**High**	**Low**

** A poll worker card (Section 5.1.4) may be required to continue polling upon the launch of the ICX application on a BMD.[72] This step was not mentioned in the researcher's report. If required, the need for a poll worker card would*

[71] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

[72] Dominion Voting Systems Corp. *Democracy Suite ImageCast X User Guide*, Aug 2018. p. 49

increase the detectability of the Safe Mode Attack and force an attacker to 1) obtain a working poll worker card and PIN, or 2) further manipulate the malicious software to bypass the card/PIN requirement.

*** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the Safe Mode Attack's feasibility are access, detectability, time, and scalability.

- **Limited Access to ICX Application.** This attack relies on access to the specific ICX software version running on Georgia BMDs for a target election. Obtaining and modifying this software may be difficult without the help of an insider or intruder.
- **Limited Access to Voting Equipment.** Testing this attack requires access to a BMD, which may be difficult without the help of an insider or intruder.
- **High Detectability.** This attack requires access to a BMD's power button, which is likely obstructed at a polling station. Moving equipment would likely be spotted by a poll worker or another voter. This physical limitation increases the likelihood that the proposed attack is performed at a county storage location (or at a precinct after hours) and requires the help of an insider or intruder with significant knowledge of the BMD and its operation. The proposed Safe Mode Attack is also detectable through an RLA.
- **Limited Time Window.** This proposed attack requires time to modify and then install the ICX application. The amount of time (and hence the number of possible modified ballots) decreases as the attack is deployed over the course of an election.
- **Limited Scalability.** Since the proposed Safe Mode Attack targets one BMD at a time, the number of potentially affected votes in a Georgia election would be statistically insignificant[73] to change the outcome of an election and avoid a recount.

5.2.5 Election Management System Attack

In a proof-of-concept attack proposed by the researcher, an EMS EDF was reportedly modified to execute ballot manipulating software when distributed to and installed on a BMD in a laboratory setting. Using an allegedly discovered vulnerability in the ICX application, the researcher asserts that they bypassed permissions and effectively gained privileged root-level execution needed to install a modified version of the ICX application.

Since BMDs run with elevated privileges, the researcher's alleged malicious EDF bypasses Android access controls and modifies a file found on BMDs that automatically executes when a BMD powers on. The modified file was described to have been programmed to swap out part of the BMD's original ICX application[74] with the researcher's ballot-altering software. The ballot-

[73] Assuming each BMD prints 225 ballots, attacking a single BMD would not have a statistically significant chance at changing the outcome of an election and avoiding a recount. In practice, MITRE NESL also assumes that this attack would be implemented in such a way to only affect a fraction of unfavorable votes to avoid detection during vote tabulation and auditing. This further increases the number of BMDs requiring an attack to change the outcome of an election.

[74] In the EMS Attack, the researcher reportedly swaps out the Ahead of Time (OAT) file in the ICX application with the OAT from the modified ICX application. OATs are commonly used in Android to efficiently launch and run applications. By

altering software allegedly changes voters' ballot selections in the printed QR codes[75] in favor of the preferred candidate.

To perform this proposed attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Modify EDF file (Section 5.1.8)
    - Obtain access to EDF file
    - Obtain access to EDF file encryption key
        - Obtain access to poll worker card and PIN (Section 5.1.4) or EMS
    - Modify the ICX application software (Section 5.1.6)
        - Obtain physical access to BMD
        - Obtain access to specific version of ICX application used in a target election
        - Obtain access and ability to use reverse engineering software
- Distribute modified EDF files to BMDs
- Possess knowledge of election related information (e.g., precinct, ballot style) specific to the ICX BMD

5.2.5.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and Georgia risk-limiting audits to determine that the proposed EMS Attack is scalable, detectable, and requires a high degree of access. MITRE NESL assessed this attack to be scalable because of its potential to affect ballots across a county. Table 10 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and definitions stated in Section 4. The values in Table 10 also assumed that the proposed attack would be performed against a single EMS (otherwise attacking multiple EMSs will increase "Time Required" and decrease "Overall Feasibility").

replacing the OAT in the ICX application, the researcher allegedly proves it possible to run a modified ICX application while leaving the original ICX application files in place.

[75] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

Table 10. EMS Attack Feasibility Matrix

Attack Component	Details	Difficulty	Time Required	Overall Feasibility
Modified ICX Application	**Access/obtain ICX software application used in a target election**	**High**	**Moderate**	**Low**
	Reverse-engineer ICX software application	Moderate	Moderate	Moderate
	Insert malicious functionality into application	High	Low	Moderate
	Repackage Application	Low	Low	High
	Access/obtain BMD hardware and software equipment for testing	**High**	**Moderate**	**Low**
Modified EDF File	**Access/obtain the original EDF**	**High**	**Moderate**	**Low**
	Access/obtain EDF encryption key	**High**	**Moderate**	**Low**
	Reform the EDF file so that it can modify BMD operating system files	Low	Low	High
	Create software that swaps out the ICX application's OAT	High	Moderate	Low
	Distribute modified EDF file to BMDs	**High**	**Moderate**	**Low**
Detectability	Attack conducted at a central county facility avoids detection by election officials (e.g., staff detects someone tampering with EMS / EDF files)	High	Moderate	Low
	Attack conducted at a Dominion facility avoids detection by Dominion (e.g., staff detects someone tampering with Election Project files)	High	Moderate	Low
	Attack avoids detection through an RLA	**High**	**Low***	**Low**
	Attack avoids detection through result tabulation[76]	Low	Low*	High
Scalability	The attack can be performed on many BMDs	Low	Low	High

** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the proposed EMS Attack's feasibility are access, time, and detectability.

- **Limited Access to ICX Application.** This proposed attack relies on access to the specific ICX software version running on Georgia BMDs for a target election. Obtaining this software may be difficult without the help of an insider or intruder.
- **Limited Access to Voting Equipment.** Testing the proposed EMS Attack requires EMS systems and BMD equipment, which may be difficult without the help of an insider or intruder.

[76] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

- **Limited Time Window.** There is a limited and decreasing time window during which an attacker can execute the proposed EMS Attack. For this attack to become scalable, the ICX software must altered and repackaged into a modified EDF before the EDF is distributed and installed on BMDs for a target election.
- **High Detectability.** The proposed EMS Attack is detectable through an RLA.

5.2.6 Infinite Voter Card / Photocopied Ballot Attack

The researcher proposes two attacks capable of producing a theoretically infinite number of ballots. Using either a photocopier or an Infinite Voter Card, the researcher reportedly produced multiple paper ballots with favorable selections in a laboratory setting. The researcher further mentions that these ballot-stuffing attacks are possible in Georgia due to the lack of a unique identifier in a ballot's QR code. The Infinite Voter Card Attack and Photocopied Ballot Attack are listed separately in the July 2021 report but were combined in MITRE NESL's analysis due to their similarity.

To carry out the proposed Photocopied Ballot Attack, the researcher asserts that an attacker can make selections on a BMD, print a ballot, and then smuggle the ballot out of the polling location for the purpose of making copies. Despite using non-standard paper, the researcher asserts that the copied ballots were all accepted by a ballot scanner. While the researcher does not discuss this step, MITRE NESL assessed that the copied ballots would need to be smuggled back into the polling location and inserted into a ballot scanner.

To carry out the proposed Infinite Voter Card attack, the researcher asserts that an attacker can create or obtain an infinite voter card, bring the card to a voting machine, print multiple ballots, and insert them into a ballot scanner.

To perform this attack, MITRE NESL assesses that an attacker must fulfill the following prerequisites:

- Obtain access to a photocopier after printing a ballot but before scanning it; or possess an infinite voting card (Section 5.1.5)
    - (Infinite voter card) Possess knowledge of Dominion's system communication protocol
    - (Infinite voter card) Obtain physical access to a BMD
    - (Infinite voter card) Obtain access to a programmable smart card
    - (Infinite voter card) Obtain access a smart card reader/writer
    - (Infinite voter card) Possess knowledge of the hard-coded PIN and Election Signature, which may also require access to a voter card or a poll worker card and PIN
- Operate in a manner at a polling station to avoid detection

5.2.6.1 Feasibility

The MITRE NESL team reviewed the researcher's documentation on the proposed attack to develop a working hypothesis of how the attack would need to be executed considering Georgia voting procedures, installation and deployment of voting equipment, verification procedures, and

Georgia risk-limiting audits to determine that the proposed Infinite Voter Card / Photocopied Ballot Attack is non-scalable, detectable, and requires minimal access. Table 11 breaks down the feasibility of the attack's components. Critical components that affected MITRE NESL's feasibility assessment are highlighted in **bold**. The values assessed by MITRE NESL assumed the criteria and definitions stated in Section 4. The values in Table 11 also assumed that the proposed attack would be performed against a single precinct (otherwise attacking multiple precincts will increase "Time Required," increase "Detectability," and decrease "Overall Feasibility").

Table 11. Infinite Voter Card / Photocopied Ballot Attack Feasibility Matrix

Attack Component	**Details**	**Difficulty**	**Time Required**	**Overall Feasibility**
Infinite Voter Card	Access/obtain real Voter Card for testing and protocol discovery	Low	Low	High
	Access/obtain BMD hardware and software for testing and protocol discovery	High	Moderate	Low
	Obtain voter card PIN	Moderate	Low	Moderate
	Obtain voter card contents	Moderate	Low	Moderate
	Create infinite voter card	Moderate	Low	Moderate
	Print multiple ballots	Low	High	Moderate
Photocopier	Send ballot photograph to accomplice for printing	Low	Low	High
	Sneak ballot out of polling location	Moderate	Low	Moderate
	Print multiple of copies of ballots	Low	Low	High
Detectability	**Smuggle printed ballots into polling location in such a way to avoid detection by poll workers, other voters**	**High**	**Low**	**Low**
	Scan multiple ballots in such a way to avoid detection by poll workers, other voters	**High**	**High**	**Low**
	Attack is conducted in such a way to avoid detection through an RLA	Low	Low	High
	Attack avoids detection through result tabulation[77]	**High**	**Low***	**Low**
Scalability	**The attack can be performed at many precincts**	**High**	**Moderate**	**Low**

** MITRE NESL assesses the noted time-required value as Low but acknowledges that the value is dependent on implementation details of the proposed attack. Because the researcher did not provide details about this aspect of the attack, MITRE NESL assumes that an attacker in this scenario has no direct involvement in the tabulating or auditing process.*

Overall Feasibility Assessment: Operationally Infeasible

The most critical factors affecting the Infinite Voter Card / Photocopied Ballot Attack's feasibility are detectability and scalability.

[77] For the purposes of this table, "result tabulation" includes state-level machine recounts and the tabulation procedure performed by election officials at precincts when polling closes.

- **High Detectability.** Poll workers are instructed to monitor a precinct's scanners as part of Georgia's standard election practices and procedures.[78] Inserting multiple ballots into a scanner as part of the proposed Infinite Voter Card / Photocopied Ballot Attack would be difficult to achieve without arousing suspicion. In addition, discrepancies between the number of voter check-ins and ballots cast would cause mismatched numbers during result tabulations in poll closure procedures. These discrepancies would be investigated and reported by election management staff. Finally, use of non-standard ballot paper types would be detectable during an audit.
- **Limited Scalability.** Both attacks are limited to a singular precinct and the copy attack can only duplicate a single ballot style unless multiple ballots are exfiltrated for copying, meaning this attack will likely only be effective in smaller scale elections.

6 Assessment of Claims

Based on the technical analysis described in Section 5, MITRE NESL assessed the researcher's claims (see Section 2) about vulnerabilities in and proposed attacks against Georgia election systems. MITRE NESL concluded that all attack scenarios described by the researcher require highly unusual opportunity, insider knowledge, technical skill, and extensive access and that it would be operationally infeasible for the attacks described on the Georgia election system to be "effectuated by malicious actors with very limited time and access to the machines" to commit "large-scale fraud" with "only moderate technical skills" in the context of changing the outcome of an election.

Table 12: MITRE NESL's Assessment of Researcher Claims - Conclusions and Rationale

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
PF.1	The researcher asserts that with access to a BMD or BMD printer, attackers can tamper with Georgia's voting equipment to change voters' selections within QR codes without their knowledge.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed QR code tampering attacks[79] are assumed to be valid; however, MITRE NESL assessed the proposed attack scenarios in which QR code tampering occurs as operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.1 BMD Printer Attack • Section 5.2.2 Technician Card Attack • Section 5.2.3 Bash Bunny Attack • Section 5.2.4 Safe Mode Attack • Section 5.2.5 EMS Attack

[78] Secure The Vote, *Poll Worker Manual 2021*. Retrieved 06 June 2022 from https://georgiapollworkers.sos.ga.gov/Shared%20Documents/Georgia%20Poll%20Worker%20Manual%202021.pdf.

[79] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
PF.2	The researcher asserts that the process used to update the ICX software on Georgia BMDs in October 2020 left the equipment vulnerable to attack.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed "Alt-Tab" attack vector that takes advantage of the vulnerability caused by the October 2020 Georgia BMD update process is assumed valid; however, MITRE NESL assessed the proposed attack scenario in which the vulnerability was leveraged to be operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.3 Bash Bunny Attack
PF.3	The researcher asserts that attackers can produce unofficial smart cards or manipulate official cards to create or enable tampering opportunities for attackers with physical access to Georgia BMDs.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed creation and use of unofficial smart cards is assumed to be a valid attack vector; however, MITRE NESL assessed the proposed attack scenarios in which unofficial smart cards were used to be operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.2 Technician Card Attack • Section 5.2.5 EMS Attack • Section 5.2.6 Infinite Voter Card Attack
PF.4	The researcher asserts that the election definition file, installed during election setup, can be exploited to deploy malicious software when installed to potentially all BMDs in a county or state.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed use of modified EDFs is assumed to be a valid attack vector; however, MITRE NESL assessed the proposed attack scenario in which the modified EDFs are used to be operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.5 EMS Attack
PF.5	The researcher asserts that using pre-installed software applications present on a BMD, attackers can gain elevated privileges which facilitate attacks and cover their tracks.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed use of pre-installed software applications on a BMD as an attack vector is assumed valid; however, MITRE NESL assessed the proposed attack scenarios in which the pre-installed applications are used to be operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.1 BMD Printer Attack • Section 5.2.2 Technician Card Attack • Section 5.2.3 Bash Bunny Attack • Section 5.2.4 Safe Mode Attack

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
PF.6	The researcher asserts that a compromised encryption key extracted from a BMD or poll worker card (with knowledge of the card's PIN) can be used to decrypt election materials across a county since the same encryption keys can be used within a Georgia county.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The researcher's proposed method of decrypting election materials from an encryption key extracted from a BMD or poll worker card is assumed valid; however, MITRE NESL assessed the proposed attack scenario in which the EDF is decrypted and modified to be operationally infeasible. MITRE NESL's technical analysis for each of the relevant attack scenarios can be found in: • Section 5.2.5 EMS Attack
PF.7	The researcher asserts that an election official with access to a ballot scanner memory card and an ordered list of voter names for that scanner can map individual voters to their ballot selections.	Associating voters with their ballot selections is not operationally possible in most precincts.	Potential voter secrecy attacks on the memory card of an ICP scanner require highly unusual access, opportunity, and knowledge. In the researcher's claim, the opportunity would be limited to small precincts with limited voter turnout. This claim assumes a poll worker can access a complete chronological list of voter check-ins and possess a means to track all individuals' voter activity throughout the voting process. In practice, this would be difficult to achieve since: 1) voters customarily check-in across multiple poll pads; 2) voters cannot be expected to cast ballots in the same order in which they checked-in; 3) multiple scanners may be available at a precinct, resulting in a distribution of ballots across multiple machines/memory cards; and 4) use of photographic and recording devices is illegal in a polling location while polls are open.[80] The claim additionally assumes that the malicious poll worker has the potential access, means, and technical skills to remove the memory card, insert it into a memory card reader, copy its contents, return the memory card to its proper storage location, and smuggle out the copied content without detection. Individuals receiving the copied content must also possess the knowledge and skills needed to parse the content. Any of these steps are technically possible in a lab environment; however, MITRE NESL assessed the execution of this proposed attack scenario to be operationally infeasible.

[80] Ga. Code Ann. § 21-2-413. Retrieved 08 June 2022 from https://casetext.com/statute/code-of-georgia/title-21-elections/chapter-2-elections-and-primaries-generally/article-11-preparation-for-and-conduct-of-primaries-and-elections/part-1-general-provisions/section-21-2-413-conduct-of-voters-campaigners-and-others-at-polling-places-generally

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
POC.1	The researcher's proof-of-concept (POC) attack involves installing a device in a BMD printer to modify ballots when they are printed.	Tampering is technically possible but is operationally infeasible to achieve in practice.	This attack scenario is operationally infeasible to change the outcome of an election due to the following factors: • Limited Access to BMD Printers • High Detectability • Limited Scalability More details about MITRE NESL's technical analysis of this proposed POC attack scenario are in Section 5.2.1.
POC.2	The researcher's POC attack involves installing software that changes votes on a printed ballot and circumvents detection on a BMD.	Tampering is technically possible but is operationally infeasible to achieve in practice.	The attack scenarios that use POC.2 are operationally infeasible to change the outcome of an election due to the following common factors: • Limited Access to ICX Application • Limited Access to Voting Equipment • Limited Time Window • High Detectability • Limited Scalability More details about MITRE NESL's technical analysis of this proposed POC attack scenario are in Sections 5.2.2, 5.2.3, 5.2.4, and 5.2.5.
POC.3	The researcher's POC attack involves a hardware device that performs automated installation of malicious software when attached to a BMD.	Tampering is technically possible but is operationally infeasible to achieve in practice.	This attack scenario is operationally infeasible to change the outcome of an election due to the following factors: • Limited Access to ICX Application • Limited Access to Voting Equipment • Limited Time Window • High Detectability • Limited Scalability More details about MITRE NESL's rationale for this POC attack are in Section 5.2.3.
POC.4	The researcher's POC attack involves a modified election definition file that installs malicious software when distributed to BMDs.	Tampering is technically possible but is operationally infeasible to achieve in practice.	This attack scenario is operationally infeasible to change the outcome of an election due to the following factors: • Limited Access to ICX Application • Limited Access to Voting Equipment • Limited Time Window • High Detectability More details about MITRE NESL's technical analysis of this proposed POC attack scenario are in Section 5.2.5.

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
MC.1	The researcher asserts that BMDs in use by Georgia are susceptible to the proposed attacks and findings. Adversaries can include foreign state and/or domestic political actors with access to Dominion equipment.	Tampering is technically possible but is operationally infeasible to achieve in practice.	Without access to Georgia's voting equipment or the researcher's proof-of-concept capabilities, MITRE NESL assumed validity of the researcher's technical capabilities. While technically possible, the researcher's proposed attacks were assessed by MITRE NESL to be operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations.
MC.2	The researcher asserts that BMDs in use by Georgia are not more secure than AccuVote Direct-Recording Electric (DRE) machines. BMDs and the associated ICX software take less time to exploit compared to AccuVote DREs.	Not enough information available to compare systems.	Without a detailed technical analysis, MITRE NESL could not assess the security of the two systems based on the analysis provided. The researcher reports that it is easier to reverse engineer the Android-based BMDs vs. the Windows CE-based DREs; however, reverse engineering only represents one of the many components in the process of a potential attack.
MC.3	The researcher asserts that the BMD-printed paper trail provides an opportunity for attackers to change voters' selections within QR codes without their knowledge. The researcher also asserts that these attacks are difficult to detect given Georgia's current risk-limiting audit (RLA) policies and practices.	Tampering is technically possible but is highly infeasible to achieve in practice.	Despite voters not being able to verify proper encoding of their selections in the printed QR code, MITRE NESL assessed the researcher's proposed QR code[81] based attacks to be operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations. Given the effectiveness of RLAs in detecting QR code based attacks, MITRE NESL assessed that RLAs should be standard practice.

[81] The QR code is considered a non-authoritative portion of a Georgia ballot. In case of audit or discrepancy, Ga. Comp. R. & Regs. 183-1-15-.04 states that "auditors shall rely on the printed text on the ballot to determine the voter's selection."

No.	MITRE NESL's Plain-language Summary of the Researcher's Claim	MITRE NESL Conclusion	MITRE NESL Rationale
MC.4	The researcher asserts that ballot-manipulating attacks can be adapted to change voters' selections in both the QR code and the plaintext portions of a printed BMD ballot. The researcher also asserts that this scenario avoids detection during RLAs. The conclusion relies on voters not reviewing their printed ballots and inconsistencies being attributed to user error.	Not enough information to assess feasibility in changing the outcome of an election.	Attackers with the access and opportunity to modify the ICX application (described further in Section 5.1.6) can technically insert new functionality into the application that changes a ballot's QR code and its plaintext. Attacks that change the QR code and plaintext avoid detection during RLAs but are detectable by voters who review their printed ballot and report discrepancies to poll workers. Poll workers document, respond to, and report these types of incidents pursuant to SEB Rule 183-1-12-.11.10. Not enough information is available for MITRE NESL to assess the feasibility for this hypothetical attack scenario to change the outcome of an election.
MC.5	The researcher asserts that Georgia assumes an increased risk of attack on its elections with its BMD-only system, where the BMDs are considered vulnerable. The researcher also asserts that other locations that use a combination of hand-marked paper ballots and optional BMDs are less likely to be attacked. BMDs in the latter scenario only print a small number of votes, which reduces attackers' incentives and potential impact.	Not enough information available to compare systems and their associated likelihood to be attacked.	Not enough information is available for MITRE NESL to assess the likelihood of attacks on the noted BMD-only and hand-marked paper ballot systems. This would require a different and additional analysis not included in this review. The required analysis would depend upon 1) data that is not known to exist at this time; and 2) baseline statistics on both identified and hypothesized compromise on paper ballots.
MC.6	The researcher asserts that Dominion's ICX software does not appear to follow modern secure software design principals and will be challenging to retrofit with security features. The researcher also asserts that despite its vulnerabilities, the ICX system was certified by programs that do not seem to be effective.	The security of Dominion's ICX software relies on operational protocols.	A complete security evaluation of the deployed systems requires incorporation of multi-layered cyber, physical, and human/operational protocols since the security of the ICX system relies on following operational procedures (many of which can be found in Appendix B). Application security risks of the ICX software can be mitigated with changes in development and deployment technical controls.

7 Conclusion

In this report, MITRE NESL performed an independent expert technical review of claims made by a researcher concerning the security of specific devices used in the conduct of elections in the State of Georgia. MITRE NESL assessed the feasibility of the researcher's proposed attacks changing the outcome of a Georgia election. Without access to Georgia voting equipment or the researcher's proof-of-concept capabilities as part of this effort, MITRE NESL assumed validity of the researcher's technical capabilities and focused on the difficulty, time-required, level of

physical access required, scalability, and detectability aspects of each proposed attack given existing compensating controls. MITRE NESL has no evidence that any of the researcher's proposed attacks, in whole or in part, have been attempted by any party in an election.

MITRE NESL observed six total attack scenarios hypothesized by the researcher and assessed each one to be operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations. Five of the proposed attacks were detectable through RLAs, as they only modified a printed ballot's QR code—a non-authoritative component of a ballot—and the sixth proposed attack was detectable during normal post-election result tabulation procedures. Five of six attacks were deemed non-scalable, impacting a statistically insignificant number of votes on a single device at a time. One attack was technically scalable but also was assessed to be infeasible due to access controls in place in operational election environments, access required to Dominion election software, and access required to Dominion election hardware.

Each of the proposed attacks requires access and/or opportunity that remains unavailable in the operational environment: all six proposed attacks require an attacker to place hands on a device, tamper with hardware and/or software, or otherwise perform actions under operating conditions and security protocols developed to prevent this form of contact with the equipment.

Appendix A: Technical Data Package Documents

The following TDP documents were made available by Susman Godfrey, L.L.P. to the MITRE NESL team:

- Democracy Suite System Security Specification (Apr 2018)
- Democracy Suite ImageCast Central User Guide (Jan 2018)
- Democracy Suite ImageCast Adjudication User Guide (Jan 2018)
- Democracy Suite ImageCast X Functionality Description (May 2018)
- Democracy Suite ImageCast X User Guide (Aug 2018)
- Democracy Suite ImageCast X System Installation and Configuration (Aug 2018)
- Democracy Suite ImageCast X System Operations Procedures (Jan 2018)
- Democracy Suite ImageCast X Software Design Specification (May 2018)
- Democracy Suite ImageCast X System Maintenance Manual (Aug 2018)
- Democracy Suite ImageCast Precinct System Hardware Specifications (Sep 2017)
- Democracy Suite ImageCast Precinct System Hardware Characteristics (Sep 2017)
- Democracy Suite ImageCast Precinct System User Guide (Jan 2018)
- Democracy Suite ImageCast Precinct Software Design and Specification (Sep 2017)
- Democracy Suite ImageCast Precinct Functionality Description (Sep 2017)
- Democracy Suite ImageCast Precinct System Maintenance Manual (Sep 2017)
- Democracy Suite ImageCast Precinct System Operation Procedures (Jan 2018)
- Democracy Suite EMS Election Event Designer User Guide (Jan 2018)
- Democracy Suite EMS Voter Activation User Guide (Jan 2018)
- Democracy Suite EMS Results Tally & Reporting User Guide (Aug 2018)
- Democracy Suite EMS Election Data Translator User Guide (Jan 2018)
- Democracy Suite EMS Audio Studio User Guide (Dec 2017)

Appendix B: Assumed Compensating Controls

MITRE NESL's list of assumed compensating controls in Table 13 were derived and adapted from recommended mitigations in the June 2022 Cybersecurity & Infrastructure Security Agency (CISA) advisory on *Vulnerabilities Affecting Dominion Voting Systems ImageCast X*.[82]

Table 13. MITRE NESL's Assumed Compensating Controls of Dominion Equipment in Georgia Elections

Compensating Control	Documentation
Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all devices, including on connected devices such as printers and connecting cables.	**O.C.G.A. § 21-2-327.** Preparation of voting machines; custodians and their deputies; inspection; furnishing of supplies **O.C.G.A. § 21-2-328.** Delivery, set up, and sealing of properly furnished voting machines prior to primary or election; protection of voting machines against molestation or injury **O.C.G.A. § 21-2-329.** Delivery of voting machine keys to chief manager. **O.C.G.A. § 21-2-375.** Delivery of equipment to polling places; protection for equipment; required accessories **O.C.G.A. § 21-2-450.** Opening of polls; procedure when ballot labels misplaced; certification by managers; machines to be locked until polls open; officers to be near machines; inspection of machines; broken machines **O.C.G.A. § 21-2-454.** Duties of poll officers after the close of the polls **O.C.G.A. § 21-2-457.** Removal, storage, and examination of voting machines after completion of vote count **O.C.G.A. § 21-2-483.** Counting of ballots; public accessibility to tabulating center and precincts; execution of ballot recap forms; procedure for torn, bent, or otherwise defective ballots; preparation of duplicate ballots **SEB Rule 183-1-12-.04.** Storage, Maintenance, and Transport of Statewide Voting System Components **SEB Rule 183-1-12-.05.** Security of Voting System Components at County Elections Office or Designated County Storage Area **SEB Rule 183-1-12-.10.** Before the Opening of the Polls **SEB Rule 183-1-12-.11.** Conducting Elections **SEB Rule 183-1-12-.12.** Tabulating Results **ICP Acceptance Test procedure and Checklist**
Ensure compliance with chain of custody procedures throughout the election cycle.	**O.C.G.A. § 21-2-327.** Preparation of voting machines; custodians and their deputies; inspection; furnishing of supplies **O.C.G.A. § 21-2-329.** Delivery of voting machine keys to chief manager **O.C.G.A. § 21-2-330.** Public exhibition of and instruction on sample voting machine **O.C.G.A. § 21-2-331.** Designation and compensation of custodians of voting machines and keys; storage of voting machines when not in use

[82] CISA, *Vulnerabilities Affecting Dominion Voting Systems ImageCast X*. Retrieved 09 June 2022 from https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01

Compensating Control	**Documentation**
	O.C.G.A. § 21-2-375. Delivery of equipment to polling places; protection for equipment; required accessories **O.C.G.A. § 21-2-377.** Custody and storage when not in use **O.C.G.A. § 21-2-379.25.** Programming for ballot design and style; verification; appointment of custodians; role of custodians; testing of electronic ballot marker; public notice of testing **O.C.G.A. § 21-2-379.26.** Storage of equipment **O.C.G.A. § 21-2-455.** Canvass and return of votes **O.C.G.A. § 21-2-485**. Responsibilities of poll officers **O.C.G.A. § 21-2-500.** Delivery of Voting Materials; presentation to grand jury in certain cases; preservation and destruction; destruction of unused ballots **SEB Rule 183-1-12-.04**. Storage, Maintenance, and Transport of Statewide Voting System Components **SEB Rule 183-1-12-.05.** Security of Voting System Components at County Elections Office or Designated County Storage Area **SEB Rule 183-1-12-.06.** Handling of Voting Systems **SEB Rule 183-1-12-.09.** Transport to Polls **SEB Rule 183-1-12-.12.** Tabulating Results **SEB Rule 183-1-12-.14.** Maintenance of Equipment **SEB Rule 183-1-12-.15.** Use of Equipment by Municipalities **COC-PM-EM-22**
Ensure a system to report irregularities observed in voting or tabulation areas.	**O.C.G.A. § 21-2-408**. Poll watchers; designation; duties; removal for interference with election; reports of infractions or irregularities; ineligibility of candidates to serve; training. **O.C.G.A. § 21-2-483.** Counting of ballots; public accessibility to tabulating center and precincts; execution of ballot recap forms; Procedure for torn, bent, or otherwise defective ballots; preparation of duplicate ballots. **O.C.G.A. § 21-2-450.** Opening of polls; procedure when ballot labels misplaced; certification my managers; machines to be locked until polls open; officers to be near machines; inspection of machines; broken machines. **SEB Rule 183-1-12-.11.** Conducting Elections
Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.	**SEB Rule 183-1-12-.05.** Security of Voting System Components at County Elections Office or Designated County Storage Area **ICX Acceptance Test Procedure and Checklist**

Compensating Control	**Documentation**
Limit physical access to all voting machines and election equipment to only persons who have "need to know" and proper authorization or supervision.	**O.C.G.A. § 21-2-330.** Public exhibition of and instruction on sample voting machine **O.C.G.A. § 21-2-379.24.** Examination of electronic ballot markers; revocation of approval; penalty to vendors for inappropriate sale; improvements or changes to devices; prohibition of pecuniary interest; limitation on public inspection **O.C.G.A. § 21-2-450.** Opening of polls; procedure when ballot labels misplaced; certification my managers; machines to be locked until polls open; officers to be near machines; inspection of machines; broken machines **O.C.G.A. § 21-2-483.** Counting of ballots; public accessibility to tabulating center and precincts; execution of ballot recap forms; procedure for torn, bent, or otherwise defective ballots; preparation of duplicate ballots **O.C.G.A. § 21-2-254.** Admission of electors to enclosed space; voting procedure generally; procedure as to write-in votes; voting by electors whose right to vote is challenged; disabled voters **SEB Rule 183-1-12-.04.** Storage, Maintenance, and Transport of Statewide Voting System Components **SEB Rule 183-1-12-.05.** Security of Voting System Components at County Elections Office or Designated County Storage Area **SEB Rule 183-1-12-.08.** Logic and Accuracy Testing **SEB Rule 183-1-12-.10.** Before the Opening of Polls **SEB Rule 183-1-12-.12.** Tabulating Results
Ensure secure transport of all voting equipment to/from polling locations	**O.C.G.A. § 21-2-328.** Delivery, set up, and sealing of properly furnished voting machines prior to primary or election; protection of voting machines against molestation or injury **SEB Rule 183-1-12-.04**: Storage, Maintenance, and Transport of Statewide Voting System Components **SEB Rule 183-1-12-.09**: Transport to Polls
Ensure all ImageCast X and ImageCast Precinct devices are subjected to rigorous pre- and post-election testing.	**O.C.G.A. § 21-2-374.** Proper programming; proper order; testing; supplies **O.C.G.A. § 21-2-376.** Demonstration of equipment **O.C.G.A. § 21-2-379.25.** Programming for ballot design and style; verification; appointment of custodians; role of custodians; testing of electronic ballot marker; public notice of testing **SEB Rule 183-1-12-.08.** Logic and Accuracy Testing **SEB Rule 183-1-12-.10.** Before the Opening of Polls **ICX Acceptance Test procedure and Checklist** **ICP Acceptance Test procedure and Checklist**

Compensating Control	**Documentation**
Encourage voters to verify their paper ballot prior to casting.	**SEB Rule 183-1-12-.11.** Conducting Elections **Secure the Vote Website:** https://securevotega.com/voting-system/ **Poll Worker Manual**: Voting Area Posters and Signs
Conduct rigorous post-election tabulation audits of the cast record portion of physical paper ballots to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures.	**O.C.G.A. § 21-2-421.** Posting of required information after closing of polls; reporting to Secretary of State **O.C.G.A. § 21-2-454.** Duties of poll officers after the close of the polls **O.C.G.A. § 21-2-455.** Canvass and return of votes **O.C.G.A. § 21-2-498.** Precertification Tabulation Audits **O.C.G.A. § 21-2-500.** Delivery of voting materials; presentation to grand jury in certain cases; preservation and destruction; destruction of unused ballots **SEB Rule 183-1-12-.12.** Tabulating Results

List of Acronyms

Acronym	Definition
APK	Android Package
BMD	Ballot Marking Device
CISA	Cybersecurity & Infrastructure Security Agency
COC	Chain of Custody
DRE	Direct-Recording Electric
EDF	Election Definition File
EMS	Election Management System
FFRDC	Federally Funded Research and Development Center
HP	Hewlett-Packard
ICP	ImageCast Precinct
ICX	ImageCast X
ISO	International Organization for Standardization
LAT	Logic and Accuracy Testing
LLP	Limited Liability Partnership
MAC	Message Authentication Code
MC	Main Conclusion
NESL	National Election Security Lab
OAT	Ahead-of-Time File
OCGA	Official Code of Georgia Annotated
PF	Principal Finding
PIN	Personal Identification Number
POC	Proof-of-Concept
QR	Quick Response
RLA	Risk-Limiting Audit
SEB	State Election Board
USB	Universal Serial Bus