# Insecurity of New Jersey's seal protocols for voting machines


## Roger G. Johnston


## October 2010

## Section 1 – Introduction

In 2008 and 2009 the plaintiffs in the New Jersey voting-machine lawsuit, Gusciora v. Corzine, asked me to study the use of tamper-indicating security seals proposed by the New Jersey Division of Elections to secure their voting machines. In this paper I am making some of my assessments available to the public.

I found that the proposed seals and security measures are *insufficient* to guarantee election integrity. The skills, time, and resources to spoof these seals and security measures are not a major barrier to an adversary, and are, in fact, widely available. The design of the AVC Advantage voting machines themselves is not conducive to good security, especially the lack of security on the voter's end of the machine. There are vulnerability and other problems with the seals chosen by New Jersey. Another serious problem is New Jersey's failure to have well-designed seal use protocols in place. The lack of internal inspections of the voting machines is unfortunate, as is the State's lack of concern about possible attacks on small numbers of voting machines (not just statewide attacks). I found that New Jersey does not exhibit a healthy security culture for elections, has no independent physical security experts and vulnerability assessors to advise the state, and misunderstands key security concepts. The poor security practices involved in storage, transport, and chain-of-custody for the voting machines are troubling as well.

Even should good seal use protocols be developed, substantial time and costs would be required to inspect the 4 different types of seals. I estimate the minimum seal inspection costs to be $266K per election, plus burdened seal procurements costs of $88K per election. Costs might well be substantially higher, and this estimate does not include other major costs, e.g., seal installation, training, and development of effective security policies.

In the remainder of this paper, numbered paragraphs correspond to similar sections of my expert report to the Court. In those sections marked with an asterisk, I have summarized corresponding paragraphs of my expert report. I omit paragraphs 1 through 11, in which I summarized my credentials, expertise, and experience, which you can find at my web site at the Argonne National Laboratory: https://blogs.anl.gov/expertsguide/roger-johnston/

The views expressed here are my own and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

**Section 2 – General Findings**

12. In my professional opinion, the tamper-indicating seals, their use protocols, and other security measures proposed by the state of New Jersey are not sufficient to detect or deter tampering with AVC Advantage voting machines. The adversary certainly needs to be motivated, willing to practice the attack, and moderately resourceful. He does not, however, need high-technology, or rare/expensive skills, tools, techniques, or materials to surreptitiously tamper with voting results.

13. Attacks on the voter panel side of the AVC Advantage also are feasible.

14. The remainder of this report is organized as follows: Section 3 defines terms used throughout this report. Section 4 presents information about seals and security vulnerabilities in general. Section 5 discusses how to judge physical security vulnerabilities. Section 6 explores a variety of concerns about New Jersey's approach to securing the AVC Advantage voting machines and to security culture in general. Section 7 presents estimates on time and costs associated with the effective use of the proposed seals. Section 8 discusses specific vulnerabilities and attacks that I have personally directed or demonstrated on the seals proposed for use on the AVC Advantage voting machines, as well as other attacks that are likely to be viable based on my considerable experience with security vulnerabilities. Section 9 discusses attacking the AVC Advantage voting machine in other ways.

**Section 3 – Terminology, Terms of Art, and Concepts**

15. "Physical security" involves protecting valuable, *tangible* assets from harm. The tangible assets can be people, buildings, machines, money, etc. The harm may include theft, tampering, sabotage, espionage, or damage. Physical security can also involve protecting *intangible* assets from harm using physical means such as guns, guards, fences, locks, safes, tags, seals, video cameras, etc. Examples of intangible assets include numerical election votes, computer data, trade secrets, communications, and intellectual property. Physical security is a distinct field of study and practice, quite different than other areas of security such as cyber (IT) security or cryptography.

16. A "lock" is a device for delaying, complicating, or discouraging unauthorized entry. It rarely stops unauthorized entry because even determined adversaries can defeat locks.

17. To "defeat a lock" means to gain unauthorized entry or access to what the lock is protecting by opening, damaging, bypassing, removing, or otherwise neutralizing the lock.

18. A "tamper-indicating seal" (often shortened to "seal") is also called a "tamper-indicating device" (TID). It is a piece of hardware or a technique for recording that unauthorized access or tampering has taken place. Unlike a lock, a seal does not resist unauthorized entry (expect perhaps in some vague psychological sense).

19. "Tampering" is gaining unauthorized access to a container or object of value for nefarious purposes of theft, damage, sabotage, adulteration, espionage, or trespassing. "Tampering" may also refer to an attack on a seal.

20. Seals are sometimes incorrectly called "tamper-resisting devices" but this makes little sense. Locks resist tampering, not seals.

21. The term "tamper-proof seal" is common but should be avoided because there is no such thing as a seal that cannot be defeated. Even if such a thing existed, it is not clear how one could prove a negative. Furthermore, a seal that cannot be tampered with is of no value. Seal users want a seal that is easy to tamper with, but also easy for the seal inspector to tell it has been tampered with.

22. "Seal installation" is the process of putting a seal on a container or object. This must be done with some care for effective tamper detection.

23. "Seal inspection" is the process of later checking the seal for evidence of tampering or unauthorized access. A seal must be inspected for evidence of tampering or unauthorized entry; otherwise, it has no security function beyond bluffing. (A lock, in contrast, provides security even if you ignore it.)

24. Seal "use protocols" are the formal and informal procedures for choosing, procuring, transporting, storing, securing, assigning, installing, inspecting, removing, and destroying seals. Other components of a seal use protocol include procedures for securely keeping track of seal serial numbers, and the training provided to seal installers and inspectors. The procedures for how to inspect the object or container onto which seals are applied is another aspect of a seal use protocol. Seals and a tamper-detection program are no better than the seal use protocols that are in place.[1-5]

25. To "defeat a seal" (unlike defeating a lock) means to fool the seal inspector. This is done by removing the original seal to gain unauthorized access to the container it is protecting, then later resealing the container with the same seal, or with a different or counterfeit seal, but without being detected.

26. Unlike a lock, simply removing a seal from a container is not defeating it, because the fact that the seal is missing or damaged will be noted at the time of inspection.

27. "Attacking" a security device (such as a lock or seal) means to undertake a sequence of actions designed to defeat it. A "successful attack" is the same thing as a "defeat".

28. "Spoofing" a security device means to defeat it in a surreptitious, undetected way.

29. A "tag" is a unique identifier of an object or container. An example is a license plate on a car.

30. Part of the confusion that is common with tamper detection terminology, even among security professionals, is that many security devices have some aspect of locks, seals, and tags simultaneously. Moreover, one kind of tag (a "security tag") but not others is essentially interchangeable with seals. And even a padlock can have tamper-detection capabilities. For example, if you were to find the lock on your storage shed smashed, you would know someone had likely gained unauthorized access, even though the padlock is a lock, not a seal *per se*.

31. A "backdoor attack" on seals involves modifying the seals in a few seconds prior to use, perhaps at the factory, vendor, or while the seals sit on a loading dock or await use. The "backdoor" which is installed compromises the seal's security. Containers, door hardware, and "hasps"—holes through which seals are inserted—are also highly susceptible to backdoor attacks.

32. "Replicating" a seal means to make a duplicate seal (with the same serial number) inside the factory, perhaps by simply ordering it, or by bribing factory personnel.

33. "Counterfeiting" a seal means to make a duplicate seal without utilizing the factory. Counterfeiting can be done by making a seal from scratch, or by using parts from authentic seals that are used or unused.

34. The “adversary” or “bad guy” (an actual term of art!) is the nefarious person who would like to tamper with the valuable assets of interest (election results in this case). The “good guys” are the protagonists who wish to prevent tampering.

35. The “insider threat” is the security vulnerability associated with the adversary being (or exploiting) the organization’s employees, contractors, vendors, consultants, or retirees.

36. “Security culture” is the official and unofficial, formal and informal behaviors, attitudes, perceptions, strategies, rules, policies, and practices associated with security. There is a consensus among security experts that a healthy security culture is required for effective security.

37. “Shannon’s Maxim”, sometimes called “Kerckhoffs’ Maxim” is a general rule of thumb in security. This maxim has held up well over the years. It is entirely consistent with my experience, and is basically common sense. The maxim states that “security by obscurity”, i.e., keeping secrets, is not an effective long-term security strategy. The adversary will eventually (usually fairly quickly) figure out the strategies, hardware, and software being deployed for security, or some insider will compromise the secret.

38. “Security in depth”, also called “defense in depth” or “layered security”, is the idea of having many security measures in place simultaneously. Sometimes this is useful for effective security, but often it creates serious, unexpected problems.[7] Using multiple seals to protect a given container or object is an example of security in depth and is subject to most of these problems. Moreover, because effective seal use protocols require a great deal of time and effort, the use of multiple seals can be particularly problematic and impractical.

39. “Ultraviolent (UV) light” is electromagnetic radiation having a wavelength between 10 nm and 400 nm. It cannot be seen with the naked eye. For seals, so called “black light” is of greatest interest. It is UV light with a wavelength around 370 nm.

40. “UV fluorescence” is a phenomenon where UV light is absorbed by a substance, then almost instantly reemitted as visible light. For seals, the excitation source is usually a black light, and the UV fluorescent ink or dye typically re-emits light in blue or green wavelengths.

41. A “borescope” is a fiber-optic imaging or viewing device used to examine the interior of wall, container, or instrument through a small hole. Borescopes are widely used by home inspectors, auto

mechanics, and others. Low-cost optical and video versions can be purchased for between $80 and $200.

42. A "man-in-the-middle attack" is an inexpensive, powerful method of attacking security devices that involves putting alien electronics along a communications path (wired or wireless). The signals are either altered, or allowed to pass through unaffected, depending on the interests of the adversary at any given time.

43. A "pressure-sensitive adhesive label seal" or "PSA seal" is a seal that looks like a sticky label. It has a serial number and often a logo. The seal is applied to the surface of interest and adheres to that surface because of the contact glue on its underside. Removal of the seal is supposed to cause some kind of change or damage that can be detected when the seal is inspected. "Lifting" a PSA seal means the seal has been removed from a surface, then reapplied without being detected.

44. A "person-day" is a unit of human labor representing one person working for 8 hours. A "burdened labor rate" is the true hourly costs of an employee including hourly wages, plus the hourly *pro rata* costs for that employee associated with benefits, work breaks, management, supervision, training, overhead, and general and administrative costs.

**Section 4 - General Comments About Seals and Security Vulnerabilities**

45. Without studying the subject of tamper detection, one might think that seals have been thoroughly perfected over the years. Unfortunately, this is not the case. In my professional opinion, physical tamper detection is a largely unsolved problem. Current seals and current seal use protocols are simply too easy to defeat using low-tech tools, methods, and supplies that are widely available to almost anyone[1-5,8-10].

46. I have studied many hundreds of seals in detail and I am unaware of any that a seal user can quickly apply to an object or container, then return later to briefly and casually examine the seal and have full confidence in being able to make an accurate determination about whether tampering has occurred or not. Casual inspection of seals is adequate to detect unauthorized access only if the adversary is not interested in surreptitious attack and just rips the seals off. Such a situation is not, however, relevant for election tampering because, by its very nature, it must be surreptitious to succeed.

47. I will discuss a number of demonstrated and feasible seal attacks in this report, but it is important to bear in mind that these are only a small subset of all possible low-tech attacks on the specific seals considered here. There are, in fact, a large number of *kinds* of seal attacks, both low-tech and high-tech.[11]

48. My Vulnerability Assessment Team and I–first at Los Alamos National Laboratory and later at Argonne National Laboratory—have shown how hundreds of different, widely used tamper-indicating seals can be defeated quickly using only low-tech tools, methods, and supplies available to almost anyone.[1-5,8-10] These seals include high-tech and low-tech seals, expensive and inexpensive seals, government and commercial seals, and electronic and mechanical (passive) seals. Even though we have the technological resources of a national laboratory available to us, we have never needed to use them to defeat even high-tech seals being used for protecting classified secrets and nuclear material. All that is required to defeat seals are low-tech attacks made with tools mostly available at a good hardware store, on the Internet, or that can be made in one's garage at home.

49. Table 1, taken from my 2006 paper in the *American Scientist* [1], shows our average results and indicates that seals do not currently provide very good security—at least the way they are currently designed and typically used.

50. Results for several hundred other seals are similar but have not yet been tabulated in Table 1.
51. Table 1 - Average results for 244 different seal designs.

| **parameter** | **mean** | **median (midpoint)** |
|---|---|---|
| attack time* | 1.4 minutes | 43 seconds |
| attack cost | $78 | $12 |
| marginal attack cost | 62¢ | 9¢ |
| time to devise a successful attack** | 12.3 hours | 12 minutes |

_____
* For one person who has considerable practice. Sometimes an assistant speeds up an attack from the times shown here.
** It may take considerably longer to practice the attack to proficiency.

52. As can be seen in Table 1, seal attacks can be fast and inexpensive (meaning low-tech). They do not require lengthy thinking to discover (as the last row demonstrates). Other seal experts have also acknowledged that current seals are easy to defeat. They have done this both in print[12-17] and via personal discussions and demonstrations in my presence. People who are not

seal experts have also devised and demonstrated successful attacks [1], including those demonstrated by computer scientist Dr. Andrew Appel with apparently relatively little effort or previous experience with seals.[18]

**Section 5 – Judging Security Vulnerabilities**

53. It is not necessary to demonstrate a perfected attack on physical security devices, systems, or programs in order to recognize the danger the attack represents, or to take prudent action to neutralize or mitigate the vulnerability. There are several reasons why a perfect seal attack is not a good standard by which to judge seal vulnerabilities. Firstly, developing an attack to perfection can be expensive for a security consultant, security expert, or vulnerability assessor, whereas an adversary may not have such high labor costs and overhead. Moreover, an adversary may be willing to devote time to developing an attack without immediate payment in anticipation of a delayed ill-gotten award should he succeed. There is no such award for a security consultant, security expert, or vulnerability assessor should she demonstrate a perfected attack.

54. It is additionally imprudent to use a perfect attack as the measure of seal vulnerability because there are many possible attacks[11]. The bad guys need only develop one successful attack. The good guys, in contrast, must be concerned with all possible attacks.

55. It is also worth noting that an adversary attacking a seal for real does not need to be perfect every time. If he botches an attempt to defeat a seal on a voting machine, he may be able to steal the machine, push it down some stairs causing major damage, run a forklift into it, vandalize it, or allow it to get in a traffic accident during moving. Any of these actions would hide his failed attempt at breaking in. (This is a viable strategy as long as the adversary does not fail too often.)

56. When considering the merits of a demonstrated attack on a seal, it is important to recognize that adversaries do not usually announce when they have attacked seals. If the testing of a seal attack involves demonstrating it (or alternatively showing a small number of seals, some defeated and some not) to an observer, that observer is fully aware that an attack has occurred. This is not a realistic test of the probability that a non-alerted seal inspector would get fooled under real-world conditions. In actual practice, an adversary almost never needs to do as thorough or

flawless a job executing a seal attack as is required in artificial tests. Real seal inspectors have many hundreds or thousands of seals to examine, not just a few. They tend to do a poor job as they get bored and tired. It is very common in the real world of seal inspection for seal inspectors to miss even blatant evidence of tampering, even assuming they are trying to do a conscientious job of inspection. (In practice, not all seal inspectors are committed *a priori* to doing a good job.)

57. Unlike defeating other kinds of security devices, defeating seals is primarily about fooling the seal inspector. Any evidence of seal tampering left after the attack is irrelevant if the inspector doesn't see it, isn't psychologically prepared to see it, or doesn't want to see it. I have studied a number of tamper detection programs where the seal inspectors do not want to report suspicious seals because of the consternation this causes their supervisor.

58. Another critical issue when judging seal vulnerabilities is the seal use protocol. Seal efficacy depends critically on details of the seal use protocol, and especially on having substantial and effective training for both seal installers and inspectors.[1-5,10,14-17,20] The training should include hands-on practice supervised by someone knowledgeable about seals and seal vulnerabilities; exercises in spotting attacks that are subtle and also attacks that are not; and detailed information about the vulnerabilities of the specific seal being used and the most likely attack scenarios. A tamper detection program that lacks good hands-on training and thoughtful use protocols will not reliably detect tampering. I have seen no evidence that New Jersey has proposed a seal use protocol, or is even cognizant that one is required.

59. In my experience, most physical security experts and security managers take the following common sense approach to judging the merits of a demonstrated attack. An attack is considered a valid threat if the attack meets most or all of the following criteria:
59a) the attack is plausible;
59b) the most critical parts of the attack are demonstrated, though not necessarily to perfection;
59c) there are no apparent provisions in the current use protocol (including training)for detecting the attack with high probability;
59d) the attack is simple, straightforward, and relatively quick;
59e) the attack can be done with common or low-tech tools and materials of modest cost that are readily available to almost anyone;

59f) the attack requires only modest skill or no skill (even if a lot of practice).
59g) attacks of this sort also work on related physical security devices, systems, or programs;
59h) the concept of the attack does not take months to devise.

60. All of attacks I have directed or demonstrated that are discussed in this report meet most or all criteria 59a through 59h, as do those I propose in this report as feasible based on my experience with seal vulnerability assessments.

61. Finally, in judging the merits of a given physical attack, it is important to be wary of using Ph.D.s to demonstrate the attack, or thinking that the person who devises an attack is the best person to execute it. For physical security attacks, or certain kinds of electronic attacks, moderately skilled technicians are often more proficient. They need not be unusually skilled or highly knowledgeable. In my experience, the average laboratory technician, auto mechanic, artist, crafts person, or wood worker can master attacks on seals more quickly than Ph.D.'s and can demonstrate better mechanical proficiency. Adversaries attacking seals and voting machines will not likely rely on Ph.D.s to actually execute the attacks (nor even need them to devise attacks). Indeed, in our Vulnerability Assessment Team, the definition that our technicians and students have long used for "attacks that are especially easy" is if Dr. Johnston can do it. (Nevertheless, I can do about half of the attacks we have developed over the years.)

**Section 6 - General Problems with the Voting Security Approach of New Jersey**

62. In reviewing the January 6, 2009 deposition [19] of Robert F. Giles, Director of the New Jersey Division of Elections, I found a number of troubling statements. In my professional opinion, Mr. Giles' views represent major barriers to having good election integrity, and show evidence of an unhealthy security culture.

63. A healthy security culture is one in which security is integrated into everyday work, management, planning, thinking, rules, policies, and risk management; where security is considered as a key issue at all employee levels (and not just an afterthought); where security is a proactive, rather than reactive activity; where security measures are carefully defined, and frequently reviewed and studied; where security experts are involved in choosing and reviewing security strategies, practices,

and products; where the organization constantly seeks proactively to understand vulnerabilities and provide countermeasures; where input on potential security problems are eagerly considered from any quarter; and where wishful thinking and denial is deliberately avoided in regards to threats, risks, adversaries, vulnerabilities, and the insider threat.

64. Throughout his deposition, but especially on pages 192-193, 245-246, and 249-250, Mr. Giles indicates that he believes good physical security requires a kind of band-aid approach, where serious security vulnerabilities can be covered over with *ad hoc* fixes or the equivalent of software patches. Nothing could be further from the truth. In my experience—indeed in the experience of most security professionals—a security device, system, or program that does not have good physical security designed in from its roots, cannot be patched up to any meaningful extent. Slapping on extra security features (including seals) after the fact does not usually work. The manufacturer or security planner needs to foresee fundamental security problems in the design stage, not try to apply fixes, countermeasures, and workarounds as an afterthought.

**65. There are other problems with Mr. Giles' security philosophy and practice as expressed in his deposition [19]:**

66. Pages 36-37: The statement from Mr. Giles that a change in the firmware does not dramatically affect the functionality (and by implication, the security) of the machine is incorrect.

67. Pages 39-40, 64-65: He demonstrates a lack of systematic approaches to security. He is not making use of either independent cyber security experts or physical security experts.

68. Pages 70, 186-187: His apparent reliance on superficial testing is a concern.

69. Pages 90, 253-254: The implication that cheating in a single election for one specific candidate is not of concern to the Director of the New Jersey Division of Elections is alarming. The idea that election fraud is acceptable as long as it is limited in scope is a surprising policy.

70. Pages 92-94: Mr. Giles' lack of understanding that a hacker does not need the source code to reverse engineer the firmware is troubling. He is confused about source code vs. assembly code vs. machine code. He fails to understand or even fully read Dr. Appel's report.

71. Page 192: This statement: “We put a security seal on a tamper evident piece of tape on that particular cartridge" shows confusion about the seals he is proposing to use. The tamper-evident tape *is* the seal.

72. Pages 194-195: Hackability is not a component of New Jersey machine testing, leaving questions of security vulnerabilities largely unexplored.

73. Pages 196-197: Mr. Giles’ uncertainty about what is actually tested on voting machines is surprising given his official position.

74. Pages 197-198: It is remarkable how much confidence Mr. Giles’ has in the security provided by seals he does not seem to fully understand, does not actually have installed, and that may not have been fully available at the date of his deposition. For example, the UV markings for the Brooks MRS2 seal and serial numbers for the ACM metal cup seals are currently lacking.

75. Pages 199-200: The idea that one failed attack demonstration eliminates the possibility that there are vulnerabilities is, in my experience, commonly found in security programs that have serious problems with cognitive dissonance. This is the mental tension between wanting to have good security and the troubling possibility that there are problems.[7] Such programs have great difficulty providing good security, or developing a healthy security culture.

76. Pages 201-205: This section demonstrates a clear lack of concern or action in regards to ballot secrecy, a fundamental voter right and a necessary ingredient for election integrity. Mr. Giles indicates he has taken no action and set no policy in regards to checking the emptiness of the ballot bags, or in dealing with the serial numbers on the paper ballots. He is not currently concerned about the latter, but notes that New Jersey “could look into it” (p 205), rather than indicating he or the state will.

77. Pages 208-209: Relying on any seal manufacturer (E.J. Brooks in this case) to choose or recommend security strategies and products for New Jersey is imprudent. More objective and independent guidance is critical, especially for end users who are not security experts. Physical security and tamper detection are serious and complex matters.[1,6-11,14,20-22] Advice should be obtained from *bona fide*, independent, objective experts on seals, tamper detection, and physical security. Similarly, relying on the manufacturer of the voting machine to suggest *ad hoc* fixes to

major security flaws in their product is problematic. If the manufacturer were proficient at understanding fundamental security vulnerabilities, they would have been unlikely to design the product with the vulnerabilities in the first place.

78. Pages 224-225: The fact that most of the seals, including the metal cup seals, the adhesive seals, and the padlock seal will essentially not be removed for extended periods of time creates four serious security problems: (1) The seals cannot be thoroughly inspected because they won't be removed for close visual examination. (2) For PSA seals, observing how the seal behaves when it is removed is the single most effective way to detect skilled attacks, and the second best way to detect unskilled attacks.[4,5] (3) The seals prevent the interior electronics from being easily inspected (including for the presence of alien electronics or rewirings), thus substantially lowering the security of the electronics. (4) Not removing the seals to gain access to the voting machine interior for inspection means that any pressure-sensitive adhesive label seals placed on the Z80 microprocessor or EPROMs have little to no role to play in security. (And without the PSA seals, the EPROMS can be fairly easily swamped out by an adversary through the "Print More" button, as explained in Section 9.)

79. Page 245: Security vulnerabilities do not "pop up" at random as Mr. Giles suggests. Rather, they are always present in large numbers whether one looks for them or not. The goal in any security program should be to proactively find as many of the easily exploitable vulnerabilities as possible, then do something about the ones that can be eliminated or mitigated.

80. Pages 250-251, 255: Regarding the insider threat, Mr. Giles demonstrates a remarkable fatalism, lack of concern, and disinterest in countermeasures.

81. Page 254: The idea that vulnerabilities have to be "proven"—whatever that is supposed to mean—rather than shown to be plausible or (better) demonstrated to some significant degree is a recipe for poor security. It is, in fact, backwards from how an effective security program and healthy security culture operates. A devised attack is an attack, whether "proven" or not.

82. Pages 272-275: It is disturbing that there is no plan, uniform site policy, or strategy for securely storing, transporting, and locking voting machines; setting up machines; or providing key security. This is not indicative of an effective security program.

83. Pages 289-290: Using third party transporters for the voting machines without doing background checks on them is ill-advised.

84. **There are also troubling signs of poor security practices and a lack of security culture present in the comments made during the depositions of James Clayton regarding Ocean County [24], Daryl Mahoney for Bergen County [25], and Elisa Gentile for Hudson County [26].**

85. Clayton, page 63: His comments do not indicate a secure and well thought-through process for protecting and retrieving seal serial numbers. Not all workers should have access to a list of all valid serial numbers on all voting machines.

86. Clayton, pages 66-68: He describes a poor chain of custody in regards to the transportation, arrival, and storage of the voting machines at the polling places and at the warehouse. There are no written policies for storage and security. Nobody watches over the voting machines at the polling places, and there is no video monitoring. Some of the voting machines in public places are not even placed in secure locations at the polling sites before and after elections.

87. Mahoney, page 32-34: Voting machines are left out in public for up to 2 weeks with little to no protection. The lack of knowledge about Finkel Trucking and why that company is chosen to transport the voting machines does not indicate a secure or well-thought through chain of custody.

88. Mahoney, page 34-36: The casual attitude about the use of temporary workers to set up voting machines and to work in the warehouse shows an unhealthy security culture and does not properly deal with the insider threat. The same is true for Mr. Mahoney's lack of knowledge about how temporary workers are chosen.

89. Mahoney, page 58-60: The keys for the voting machines are kept with each machine in the warehouse, where temporary workers interact with them. There is no pre-authorization for a technician to work on a voting machine. These practices show an unhealthy security culture and a lack of concern for the insider threat.

90. Gentile, pages 63-67: These comments also show an unhealthy security culture. It is troubling that Ms. Gentile lacks knowledge about the company and its employees who do the election tests, why the company was chosen, or whether the company runs background checks on its employees. The fact that unfamiliar

personnel may be part of the work crew is also problematic for good security.

91. Gentile, pages 89-91: There is a similar lack of knowledge and interest in how and why the voting machine movers were chosen. The fact that the workers can randomly vary, and that they ride in the back of the truck with the voting machines is not a good security practice.

92. Gentile, pages 91, 93-95: The lack of documentation and a formal chain of custody for the transport, delivery, and acceptance of the voting machines represents poor security practice. At times, there is no one present to accept the voting machines at polling places and be sure they are well cared for. The fact that Ms. Gentile does not know if the movers have had background checks is also disturbing.

93. **Given limited security features built into the AVC Advantage voting machine, the absence of a healthy security culture for New Jersey elections, and New Jersey's lack of well designed seal use protocols, I believe there are viable attacks on New Jersey voting machines that are limited in scope but still capable of affecting election results. It is imprudent to assume that adversaries would need to attack hundreds or thousands of voting machines, strive to tamper with election results for more than 1 election at a time, or automatically try to rig voting for more than one candidate. New Jersey has historically had a number of remarkably close elections, as the Public Advocate has pointed out[27,28]. For these elections, tweaking the results in 1 or 2 key precincts could have resulted in candidate B falsely appearing to defeat candidate A. Common sense suggests that the desire to rig an election is correlated with how controversial the election is. This, in turn, is correlated with how close the election is likely to be, which is correlated with how few fraudulent votes will be needed to cheat. In other words, adversaries are likely to find it easiest to rig the elections and the results for candidates that they care most about.**

94. It is my professional experience that firmware does not have to be fully reverse-engineered and the source code fully reconstructed in order to tamper with the performance of an electronic device or system. It is undoubtedly true that fully reverse-engineering microprocessor code allows for the most thorough and difficult to detect attack, and one that could operate well into the future. Doing this, however, takes more time and skill than is needed to hijack the performance of the device or system at a more modest level. A brief analysis of the microprocessor code, along with an empirically derived study of

the device functionality can often be used to make an alien microprocessor mimic the performance of the original device sufficiently to fool the device user.

95. It is my experience that so-called "security in depth" can be highly problematic.[7] Typically, organizations with poorly thought-through security often pile on multiple security features, devices, or layers in hopes that the complex interaction of all these layers will somehow automatically add up to good security. This rarely happens. New Jersey's use of multiple seals is clearly an example of security in depth that is neither well thought-through, nor likely to be successful.

**Section 7 – Time and Costs for Effective Seal Protocols**

96. In my professional opinion, seal installers and inspectors using mechanical seals require a minimum of 12 hours of hands-on training per year for each type of seal they are using in order to reliably detect moderately skilled, low-tech attacks. (Detecting highly skilled low-tech attacks, or high-tech attacks at almost any skill level would require even more training.) Training must include seeing seal attacks and working with seals that have been defeated both with great sophistication and without.

97. The time and costs involved in inspecting all the seals that New Jersey proposes to use on the back end of the AVC Advantage voting machine is substantial. As discussed in paragraph 78 above, the seals should all be removed after each election from each voting machine for reliable tamper detection. Doing this is also required to examine the interior electronics. I estimate the time for seal removal & inspection (including checking the serial number), removing the screws on the sheet metal covers, interior electronics inspection, then reinstalling the sheet metal covers, reinstalling the seals, and recording the new seal serial numbers seals at 12 minutes per voting machine. For 11,000 voting machines, this represents 275 person-days, respectively per election. At a fully burdened labor rate of $50/hour, this represents $110K per election.

98. In my professional opinion, good voting security requires removing, then inspecting each of the 12 (subpanel) printed circuit boards inside the voters panel to look for modifications and alien electronics. Viable voter panel attacks are described below in Section 9. I estimate the costs of inspecting all 12 subpanels of the AVC Advantage voting machine for tampering with the electronics at 13 minutes per machine, or (for 11,000 voting

machines) 298 person-days = $119K per election under the same assumptions.

99. The top, sides, and bottom of the voting machines need to be examined to detect cutting or drilling and subsequent repair (or replacement of the entire voting machine case). A careful examination needed to spot an adversary's good repair job requires approximately 4 minutes in my experience. For 11,000 voting machines, this represents 92 person-days or another $37K per election under the same assumptions.

100. My estimate of the total costs of providing effective inspection for 11,000 AVC Advantage voting machines thus equals $110K + $119K + $37K = $266K per election. This estimate does not include the potentially larger costs associated with buying the seals, developing a specification and procurement process, installing the seals, securely storing the seals, buying the tools needed for the work, maintaining a secure serial number data base, developing a secure disposal process for the used seals, properly training seal installer and inspectors (discussed above), and developing effective security policies. I estimate the cost of procuring the seals (including overhead & security protocols) at about $8 per voting machine. This represents an additional $88K per election for 11,000 voting machines.

101. The estimated task times and costs in the above paragraphs, assume (1) motivated workers who (2) are experienced at the task. If one or both of these two assumptions are not valid, the times and costs will be greater by a factor of 2 or 3 then estimated here. Note also that a single voting machine can be inspected much more quickly than the times estimated above, but that pace and the quality of the inspection cannot be maintained by hourly workers for extended periods of time.

102. It should be noted that the cost per election would be greater if the fully burdened labor rate exceeds the $50/hour assumed here. In my experience, the fully burdened labor cost for a technician at federal facilities, for example, is typically $80/hour to $200/hour.

## Section 8 - Specific Seal Vulnerabilities & Attacks (Demonstrated & Feasible)

E.J. Brooks Padlock Seal

*103. A simple method that uses inexpensive tools can open and reclose the Brooks Padlock seal in about a minute. The seal can be reused with no apparent damage or evidence of tampering. With sufficient skill and practice, this attack could probably be performed in less than 15 seconds.


Figure 1 – The E.J. Brooks padlock seal.

*104. I have also demonstrated that it is easy to counterfeit the seal, by purchasing a fresh seal and changing its serial number to match the seal to be attacked.

Figure 2 - A $144.95 illuminated borescope available at Amazon.com.[29]

105. If the adversary does the printing offsite, the total attack time spent at the voting machine to defeat the padlock seal is the time to note the serial number, then return later to remove the original seal and replace it with the counterfeit, or about 6 seconds total onsite.

106. Other attacks on this seal are no doubt possible (because I have defeated similar seals in other ways) but either of the above two attacks, or the one demonstrated by Dr. Appel[18], would be sufficient to fool the seal inspector under ordinary conditions.

E.J. Brooks Ring Pull II Bidirectional Plastic Strap Seal

*107. I have demonstrated how to open and reclose this seal in a few seconds using everyday materials. I also describe three other modes of attack on this seal.


Figure 3 – The ACM Model 3001 plastic strap seal.[54]

American Casting and Manufacturing *MCS-C Cup Seal*

108. A phone call to American Casting and Manufacturing (ACM) verified that the company is no longer manufacturing the MCS-C Cup Seal. ACM will cease selling it when the modest supply on hand is sold out. Moreover, ACM will not provide any imprinted lettering or serial numbers for the limited stock on hand. With no unique identifier, this product is not technically a seal and cannot *a priori* provide effective tamper detection.

*109. I have directed many different kinds of defeats of metal cup seals of this kind. The attack takes only seconds and leave no apparent damage.

*110. I have done this attack personally, but certain members of my Vulnerability Assessment Team are more skilled, and have completed the attack in less than 35 seconds.

111. In my view, the attack demonstrated by Dr. Appel [18] is also a viable attack.


Figure 4 – The American Casting and Manufacturing MCS-C Cup Seal. From reference [31]. The bottom portion of the seal (center, with the screw hole) has a diameter of ~0.490", while the cap (left and right) has a diameter of ~0.464".

112. Even if a serial number were to be applied to the MSC-C Cup Seal, reading the serial number would be challenging for the seal inspector. This is because of the requisite small size and nature of the stamping on the cap. The serial number would be difficult enough to read if you hold it up close to your eye and get the reflected illumination just right. Reliably reading it from a distance while it is mounted inside the voting machine is going to be time consuming and challenging. Seal inspectors do not perform well when the task is difficult.

*113. I can describe at least two methods for counterfeiting this seal. I know from past experience that the latter is easy and fairly inexpensive because I have personally directed this kind of attack on similar seals.

*114. There are other problems with this cup seal that compromise its security.

*115. There is yet another problem that compromises the security of this cup seal. This is a common problem for seal manufacturers who sell in volume.

MRS2 Pressure Sensitive Adhesive (PSA) Seals

116. The MRS2 adhesive label seal (figure 5) with a custom visible logo and ultraviolet logo currently belongs in the category of seals that could theoretically exist but either don't exist or aren't currently available from the manufacturer (though they may be at some point in the future). In general, judging the merits of attacks on such "potential" seals is problematic because

the efficacy of seals depends critically on the details and on studying actual seals. Nevertheless, it is clear that this seal has multiple problems for use on the AVC Advantage voting machine.

117. Pressure-sensitive adhesive (PSA) label seals do not usually provide reliable tamper detection.[2,4,5,8,12,13,15] I have examined the Brooks/Markitwise MRS2 Seal proposed for use on the AVC Advantage voting machine. In my professional opinion—having carefully studied hundreds of different PSA seals over 16 years—the MRS2 seal does not provide high-levels of security. Indeed, it is even easier to defeat than many other PSA seals.

Figure 5 – The MRS2 PSA Seal[32,33]

*118. I have found the MRS2 seal easy to remove without damage if one is careful. In my expert report to the Court I described the methods in detail.

*119. I describe other methods to remove this seal without damage to it, so it can be replaced with no evidence of tampering.

120. The use of "secret" UV markings on this seal—or any other PSA seal for that matter—contributes nothing significant to security. There are multiple reasons for this:

121. Shannon's Maxim says that keeping secrets is not an effective long-term security strategy.

122. Almost anyone sufficiently familiar with seals knows that ultraviolet (UV) markings are common on seals and security documents. Moreover, anyone interested in the MRS2 seal (such as adversaries interested in spoofing it) are likely to view the web pages for E.J. Brooks (as Dr. Appel has pointed out) or Markitwise (the actual manufacturer of the seal[32,35]). Both web sites discuss UV marking of seals. Both sell UV pens and inks.[36-39] See figure 6. I do not know for sure because I have not viewed these particular inks or run a spectroscopic analysis, but it is likely they employ the same UV inks (or something quite similar) proposed for the MRS2 seals.

123. The general public has known about UV inks and paints, and black lights that make them visibly fluoresce since the 1960's.[40] As figures 7 and 8 demonstrate, inexpensive black lights are sold to consumers. So called "spy pens" using UV ink and a black light are available as novelties and sold as children's toys.[41-44]. See figure 9. UV pens are available to home owners to mark their property.[36,39] See again figure 6. Many machinists, auto mechanics, and mechanical technicians know that the tools in their workplace are marked with ultraviolent inks for identification purposes. Ultraviolet inks are readily available for sale to the public [45-47] in a variety of different fluorescence emission colors [48], and the colors can typically be tweaked a variety of ways, including by changing the pH (acidity). The public can even buy computer printer cartridges for printing with UV ink using standard computer printers.[49,50]


Figure 6 – The E.J. Brooks UV marking pen advertized on their web site.[39]

Figure 7 - Walmart's 18" black light for home use.[40] According

to the Walmart.com web site, this $21.88 black light will help you "bring back the 60's and 70's with the ever popular black light."

Figure 8 - One of several 75-watt UV light bulbs available from Amazon.com for a few dollars.[29]


Figure 9 - The "Kids Spy Pen - Ultraviolet Spy Pen" available from [41] for $3.95 and sold through Amazon.com [29] for "ages 3 and up". The pen writes with UV ink, and has a battery-powered UV light on the other end to make the invisible writing fluoresce. Essentially the same product is sometimes available from surplus, novelty, and toy vendors for $1.95.

*124. A semi-skilled artist, graphic artist, craftsman, hobbyist, or technician can replicate the UV markings in any of several different ways. And because the UV illumination used to examine seals is typically uneven spatially, and because the seal's UV fluorescence is relatively dim, it is usually difficult for the seal inspector to

see the UV patterns clearly. This means that the counterfeit UV pattern does not typically have to be of good quality.

*125. I describe yet another way to counterfeit UV markings.

126. The advantage of counterfeiting seals for the adversary, of course, is that almost all the work is done at his home base. He can just cut the original seals off the voting machine and replace them quickly with counterfeits

127. The ostensible purpose of a secret UV mark is to serve as a countermeasure to seal counterfeiting. But lifting, not counterfeiting, is the easiest and most likely attack on these (and most other) PSA seals. Moreover, an "invisible" logo and/or lettering on just part of the seal does not prevent seal counterfeiting involving reuse of all or part of a legitimate seal.

128. E.J. Brooks and Markitwise are planning to sell the MRS2 seal to the general public, making partial seal counterfeiting through use of an existing seal particularly easy.

*129. As an example of a partial counterfeit attack, I have demonstrated that the serial number on the MRS2 seal can be changed without damaging the seal or leaving any obvious evidence. This obvious vulnerability has been known for PSA seals in general since the 1970's.[21] Thus, access to a MRS2 seal, either purchased from E.J. Brooks or stolen from the New Jersey election supply, would allow an adversary to create a convincing counterfeit seal.

Previous Seals

*130. It is my understanding that New Jersey has previously proposed using other seals on the AVC Advantage voting machines. All of these that I am aware of can also be defeated fairly easily. I have, for example, previously defeated the Multi-Lok Cable Seal (see figure 10) in just a few seconds. This attack leaves no evidence. Unlike Dr. Appel's attack [18], this attack does not require drilling any holes or disassembling the seal. His attack, however, would be successful, in my experience, in fooling seal inspectors.


Figure 10 - The Brooks Multi-Lok Cable Seal.[23]

*131. I have also demonstrated how plastic strap seals (figure 11) can be opened in a few seconds using everyday materials.

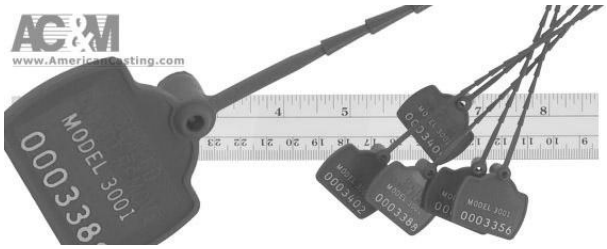


Figure 11 – The ACM Model 3001 plastic strap seal.[30]

**Section 9 – Other AVC Advantage Security Problems**

Opening the AVC Advantage Door

132. Dr. Appel has demonstrated picking the lock on the AVC Advantage voting machine back door. Rather than picking the lock, however, (should a better lock be applied), there is another way to open the door that takes even less skill. The 1/8" steel center pin in the hinge can be pushed out (as I have demonstrated), allowing the door to open without disturbing the lock. This, despite the fact that the hinge is mounted internally. (There is a large gap between the door and the voting machine, allowing access to the hinge center pin.) The original center pin, or a full or partial replacement pin can be put back with no

evidence of access. This method of opening the door is slower than picking the current lock and makes much more noise, but takes less skill. In general, it makes little sense to lock or seal a door when the hinge or hinge pin can be easily removed.

Swapping out the EPROMS

133. If no PSA seals are applied to the EPROMs, it is relatively easy for an adversary to swap them out. The blue "Print More" button switch (figure 12) on the power up panel inside the AVC Advantage can be pulled out by hand, leaving a hole through which a bent wire can be used to remove, then later replace one or more of the EPROMS. This takes a little bit of skill and typically about 1-2 minutes based on my experience with the AVC Advantage voting machine, though it would no doubt be much faster with practice.

134. A PSA seal applied to the EPROMS would make this attack difficult, though those seals must be inspected in order to have any useful role to play in security. Reliably inspecting those seals would require a partial disassembly of the voting machine, as discussed in the portion of Section 7 about costs.

135. It may be even easier and faster to swap out the EPROMs if the power panel (figure 12) is removed first. This would require defeating any seal applied to the panel.

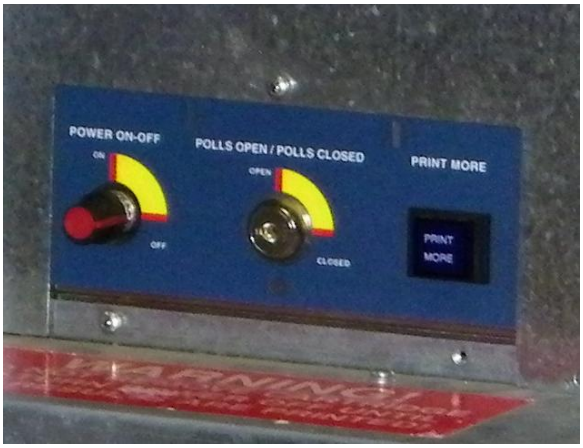


Figure 12 - The blue "Print More" button(right)can be pulled out by hand, allowing nearby access to the EPROMs.

Swapping out the Z80 Microprocessor

136. I observed an engineer with my Vulnerability Assessment Team remove the Z80 microprocessor from an AVC Advantage voting machine using a $155 hot-air soldering iron. This took 85 seconds on the first try. It was done from the front of the motherboard without removing the motherboard.

137. The time to resolder the Z80 microprocessor back in place was 93 seconds on the first try. Practice would probably reduce the soldering and desolding times to under 40 seconds for each. These times do not include the time to remove and reinstall any adhesive label seals on the microprocessor.

Voter Panel Attacks

138. Dr. Andrew Appel has focused on the concept of attacking the proposed AVC Advantage seals in order to gain undetected access to the Z80 microprocessor and/or the EPROMs.[18] This would allow the adversary to hijack the performance of the AVC Advantage voting machine. I agree that this is an attack that is both likely to succeed and very devastating because of the long-term ability for an adversary to control the voting machine well into the future without being detected.

139. A different set of attacks are possible from the voter's end of the AVC Advantage voting machine. The simplest attack, which I will call the "paper swap attack" is for a voter early in the voting to swap the large paper sheet on the voter's panel showing the candidates names, using a rolled up substitute hidden down one leg of his pants. His attack would be hidden by the privacy curtain. A second voter could swap the paper back later the same election day to hide evidence of tampering, though this wouldn't be necessary if there is no testing or close inspection of the voting machine within a few weeks of the election.

140. This attack is possible because it is my understanding that New Jersey publicizes the position of each candidate's name on the ballot well in advance of the election. This paper swap can be done behind the privacy curtain by removing a few screws in less than 30 seconds. No security features prevent this swap.

141. The paper swap attack requires 2 dishonest, registered voters (or 1 corrupt poll worker) per tampered voting machine. This attack is thus less efficient than the man-in-the-middle attack discussed below, but it might still be viable in very close elections if the poll locations to attack were cleverly chosen.

142. Other types of voter panel attacks are electronic in nature. These attacks are straightforward because—surprisingly—the voter has easy access to the electronics on the voter end of the AVC Advantage voting machine, yet these electronics are rarely if ever inspected[19,24-26]. Equally surprising, there is no tamper switch to detect opening of the voter's panel.

143. These electronic voter panel attacks require no reverse-engineering of the Z80 microprocessor code, swapping of EPROMS, or attacks on seals. They do not require much sophistication because the voter panel electronics on the AVC Advantage voting machine involve only easy-to-figure-out digital logic without a micro-processor.

144. These electronic attacks can be executed by a registered but nefarious voter (hidden by the privacy curtain), or—more likely—by a nefarious adversary working on the voting machine while in storage or transit. In either case, the adversary need only remove a few screws (and perhaps the voting paper sheet with the candidates' names)in order to gain access to the voting subpanels.[53]

145. The simplest voter panel electronic attack, **which I and my Vulnerability Assessment Team have demonstrated on version 5 of the AVC Advantage voting machine**, involves stealing votes for one or a few candidates. I call this the "modify attack". The adversary needs only to swap out one printed circuit board (subpanel) with another that has a few electrical connections changed. Alternately, he can modify one or more subpanels in place with a pen knife and a battery-powered or butane-powered soldering iron.

146. The modified wiring for this "modify attack" is done such that the lights on the voting panel continue to operate correctly for future voters, but their votes don't register for the correct candidate(s). The fact that the Z80 microprocessor basically drives the lights on the voter panel is not a problem when the subpanel printed circuit board is modified properly, as we have shown.

147. I do not know if the modify attack will work on the latest version of the AVC Advantage voting machine. If not, the attack will need to be slightly changed. It is my understanding that New Jersey has refused to make available to me the Sequoia Advantage version 9.00H, currently in use in New Jersey, and that the Court has held that it would be acceptable for me to instead examine a version 5 unit for the purposes of evaluating vulnerabilities.

148. There are a number of ways for an adversary to obtain a subpanel to modify if he does not wish to modify the subpanels on site. Replacement subpanels can be purchased inexpensively.[53] Alternately, an entire used voting machine can be purchased from the Internet, a subpanel can be taken from an unused voting machine in the warehouse, or (perhaps) an unused subpanel can be borrowed from the working voting machine after the startup sequence. The subpanel swap takes about 20 seconds with practice, not counting the time to remove and replace the voter panel paper (if necessary). Alternately, the original subpanel can be modified in a minute or two (even behind the privacy curtain during voting)with considerable practice.

149. A more surreptitious subpanel attack than the "modify attack" is to modify the subpanel such that the vote tampering can be turned off or on. I will call this the "on/off attack". This attack can be done remotely a number of different ways, including with an inexpensive microchip radio frequency receiver such as used by electronics hobbyists. My Vulnerability Assessment Team and I have demonstrated this kind of remote control on/off attack on a variety of other types of security devices.

150. An alternative to remote control of the voter panel tampering is to let the adversary's microprocessor decide if a voting test is underway and suspend tampering with election results if it is. A voting test might be detected based on any number of parameters including the date and time (the micro-processor circuit would have a clock), use of a small solid-state accelerometer indicating the voting machine had just been rolled somewhere, or by detecting the artificially fast button selection that likely occurs during voting testing.

151. If the adversary wants to hijack the complete election for an entire voting machine, and not just tamper with candidates on a single subpanel, he can do a full blown "man-in-the-middle attack". This requires a $1 microprocessor with a battery. The microprocessor would feed the Z80 microprocessor (from the voter panel side) either the correct voter button settings (when off), or false settings (when on). Because the voter panel electronics are essentially never inspected, this man-in-the-middle attack can lay in wait for the next election indefinitely. It would be reprogrammed for a new election remotely using radio frequency communication.

152. Even if inspection of the voter panel electronics were to occur, I know from personal experience that the use of surface-

mount electronics can make the alien electronics difficult even for a knowledgeable electronics technician to spot.

153. I am in the process of developing the remotely controlled on/off and man-in-the-middle attacks described above for the AVC Advantage voting machine. I do not know if there will be sufficient time to develop and then demonstrate these attacks given my schedule. Not being allowed access to the latest model of the AVC Advantage voting machine means I cannot be certain that these attacks would work. If the design has been changed dramatically in the new model, these attacks would require modification.

**Section 10 - Summary**

154. In summary, I can state to a reasonable degree of certainty that the seals and security measures proposed by New Jersey to provide security for the AVC Advantage voting machines are insufficient to guarantee election integrity. The skills, time, and resources to spoof these seals and security measures are not a major barrier to an adversary, and are, in fact, widely available.

155. Various factors contribute to New Jersey's ineffective security. The design of the AVC Advantage voting machines themselves is not conducive to good security, especially the lack of security on the voter's end of the machine. There are vulnerability and other problems with the seals chosen by New Jersey. Another serious problem is New Jersey's failure to have well-designed seal use protocols in place. The lack of internal inspections of the voting machines is unfortunate, as is the lack of concern about attacks on small numbers of voting machines given the number of close elections in the past.

156. Other negative factors include New Jersey's failure to exhibit a healthy security culture for elections, the absence of independent physical security experts and vulnerability assessors to advise the state, and the state's misunderstandings about key security concepts. The poor security practices involved in storage, transport, and chain-of-custody for the voting machines are troubling as well.

157. Even should good seal use protocols be developed, substantial time and costs would be required to inspect the 4 different types of seals. I estimate the *minimum* seal inspection costs to be $266K per election, plus burdened seal procurements costs of $88K per election. Costs might well be substantially higher, and this

estimate does not include other major costs, e.g., seal installation, training, and development of effective security policies. None of these costs would directly address the serious vulnerabilities of the voters panel.

**Documents Cited in This Report**


1. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94**(6), 515-523 (2006).

2. RG Johnston, ARE Garcia, and AN Pacheco, "Efficacy of Tamper-Indicating Devices", *Journal of Homeland Security*, April 16, 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

3. RG Johnston and ARE Garcia, "Simple, Low-Cost Ways to Dramatically Improve the Security of Tags and Seals", *Proceedings of the IAEA Symposium on International Safeguards*, Vienna, Austria, October 13-17, 1997.

4. RG Johnston, "Some Comments on Choosing Seals & on PSA Label Seals", Talk for the $7^{th}$ *Security Seals Symposium*, Santa Barbara, CA, February 28-March 2, 2006 (Los Alamos National Laboratory Document LAUR-06-0943).

5. RG Johnston, "The Real Deal on Seals", *Security Management* **41**, 93-100 (1997).

6. EG Bitzer, PY Chen, and RG Johnston, "Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology", *Industrial and Organizational Psychology* **29** (in press).

7. RG Johnston, "Layered Security: Self-Defense or Self-Delusion?", *Security Management* (in press).

8. RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues* (in press).

9. RG Johnston and JS Warner, "The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", Security Management **49**(9), 112-121 (2005).

10. RG Johnston, "Tamper Detection Requires Dedication", *Metering International*, issue 3, (1999), http://www.metering.com

11. RG Johnston and ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **229**, 23-30 (2000).

12. JL Rosette, *Improving Tamper-Evident Packaging: Problems, Tests and Solutions*, 1992

13. H Lockhart and FA Paine, *Packaging of Pharmaceuticals and Healthcare Products*, Springer (1996).

14. DC Ruriani, "Selecting the Right Cargo Security Seals", *InboundLogistics*, May 2006, http://www.inboundlogistics.com/articles/10tips/10tips0506.shtml

15. *DoD Seals Training Course*, Port Hueneme, California; Naval Facilities Engineering Services Center, https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks

16. *DoD, Antipilferage Seal User's Guide*, Port Hueneme, California; Naval Facilities Engineering Services Center, https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks

17. DL Poli, *Security Seals Handbook*, Report SAND78-0400 (Albuquerque, New Mexico; Sandia National Laboratories, 1983.

18. Andrew W. Appel, Certification of December 1, 2008, including Seals Demonstration Video.

19. Deposition of Robert F. Giles, January 6, 2009, Docket No. L-2691-04.

20. US Nuclear Regulatory Commission, Regulatory Guide 5.15, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material", March 1997, http://www.orau.org/ptp/PTP%20Library/library/NRC/Reguide/05-015.PDF

21. US Atomic Energy Agency, Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material, July 1973.

22. R Anderson, *Security Engineering*, Wiley (2008).

23. E.J. Brooks, *Multi-Lok Cable Seal*, http://www.brookseals.com/catalog/product-detail.asp?ID=35

24. Deposition of James Clayton.

25. Deposition of Daryl Mahone.

26. Deposition of Elisa Gentile.

27. New Jersey Department of the Public Advocate, "Close Elections in New Jersey and Their Significance for the Behavior of Eligible Voters and Election Officials", October 27, 2008, http://www.state.nj.us/publicadvocate/public/pdf/close%20elections%20article%20v6.pdf

28. "Recent Close Elections in New Jersey", http://www.state.nj.us/publicadvocate/public/pdf/ByCountyCloseElections.pdf

29. Amazon.com.

30. American Casting and Manufacturing, *Model 3001 Plastic Strap Seal*, http://www.americancasting.com/info-plastic-strap-seals-3001.asp

31. American Casting and Manufacturing, *Model MCS-C Cup Seal*, http://www.acmseals.com/images-cup-seals-SCS-S.asp

32. Markitwise, *Type MRS2*, http://www.markitwise.co.uk/security-seals/type-mrs2

33. E.J. Brooks, *Type MRS2 Tamper Evident Label*, http://www.brookseals.com/catalog/product-detail.asp?ID=747

34. Markitwise, *Type MRP2, high tack rubber based adhesive*, http://www.markitwise.co.uk/security-seals/type-mrp2

*35. Brooks Consolidates UK OPs*, Sept 2007, http://www.worldcargonews.com/htm/n20071019.948445.htm

36. Markitwise, *Cycle/Home & Mobile Phone Multi-Pack Security Marking Kits*, http://www.markitwise.co.uk/property-marking/cycle-home-multi-packs

37. Martkitwise, *U.V. (Invisible) Marking & Protection*, http://www.markitwise.co.uk/property-marking/ultra-violet-marking

38. EJ Brooks, *UV Property Marking Kit*, http://ejbstorefront.ejbrooks.com:80/brookstore/product.asp?category=192&part%5Fno=9560000&find%5Fcategory=WEB%5FALL&find%5Fdescription=all+products&find%5Fpart%5Fdesc=

39. EJ Brooks, *Tamper Indicative Labels, Tapes, and Anti-Counterfeit Products*, http://ejbstorefront.ejbrooks.com:80/brookstore/product.asp?category=192&part%5Fno=9560000&find%5Fcategory=WEB%5FALL&find%5Fdescription=all+products&find%5Fpart%5Fdesc=

40. Walmart.com, *Black Light*, http://www.walmart.com/catalog/product.do?product id=8198021

41. *I Spy Pen*, http://www.landofnod.com/family.aspx?c=8098&f=4919

42. US Toy, *Invisible Ink Pen with Blacklight*, http://www.ustoy.com/cgi-bin/ustoy cgi.sh/WService=ustoy/ustoy.com/novelty/product.htm?stateInfo=?&dept id=151&pf id=MX56&utm source=froogle&utm medium=free&utm campaign=Updated20090130&utm term=CV

43. *Invisible Ink Pen Kit*, http://www.target.com/dp/0762425075/sr=1-1/qid=1233453453/ref=sr 1 1/185-6881609-2312460?ie=UTF8&index=target&rh=k%3Aspy%20pen&page=1

44. Amazon.com, *Children's Invisible Ink Fairy Diary*, http://www.amazon.com/Childrens-Invisible-Ink-Fairy-Diary/dp/B001IPOJDU

45. Castleink, *Invisible Inks*, http://www.castleink.com/ a-invisible-inks.html

46. *Invisible Ink Kit*, http://www.azstamps.com/ProductDetail.aspx?productid=INV KIT

47. *Stamp Design Wizard*, http://www.azstamps.com/AutoStamp.aspx?catid=8

48. Globright, *Multi-color UV inks*, http://www.globright.com/invisibleink.html

49. Hewlett Packard, *UV/IR Invisible Ink Print Cartridge*, http://www.hp.com/oeminkjet/reports/4AA0-5780ENUC.pdf

50. *Versaink Invisible Fluorescent UV Ink*, http://www.g7ps.com/scripts/versainkuv.asp

51. Silk Screening Supplies. Com, http://www.silkscreeningsupplies.com

52. *Heat Transfer Papers*, http://www.prodistributors.com/list.html

53. JA Halderman and AJ Feldman, *TR-816-08, AVC Advantage: Hardware Functional Specifications*, March 2008, http://www.cs.princeton.edu/research/techreps/TR-816-08

54. E.J. Brooks, *Ring Pull II Seal*, http://www.brookseals.com/images/product/pdfs/RingPull-II.pdf