Exhibit 31

Report Information from ProQuest

July 12 2017 17:47

Table of contents

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 1

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.
ProQuest document link

Links: Check SFX for Availability

Full text: (CORRECTED COPY - CORRECTIIONS THROUGHOUT TEXT)
S Intel Hearing on Russian Interference in 2016 Election, Panel 1
JUNE 21, 2017
SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.
SEN. ANGUS KING, I-MAINE
SEN. JACK REED, D-R.I.
WITNESSES: SAM LILES, ACTING DIRECTOR, OFFICE OF INTELLIGENCE AND ANALYSIS CYBER DIVISION DEPARTMENT OF HOMELAND SECURITY
JEANETTE MANFRA, UNDERSECRETARY OF HOMELAND SECURITY, AND ACTING DIRECTOR, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
BILL PRIESTAP, ASSISTANT DIRECTOR, FBI COUNTERINTELLIGENCE DIVISION
[*] BURR: Today the committee -- committee convenes it's sixth open hearing of 2017, to further examine Russia's interference in the 2016 elections. This is yet another opportunity for the committee and the American people to drill down on this vitally important topic.
In 2016 a hostile foreign power reached down to the state and local levels to touch voter data. It employed relatively sophisticated cyber tools and capabilities and helped Moscow to potentially build detailed knowledge of how our elections work. It was also another example of Russian efforts to interfere into a democracy with the goal of undermining our system.
In 2016, we were woefully unprepared to defend and respond and I'm hopeful that we will not be caught flatfooted again.
Our witnesses are here to tell us more about what happened in 2016, what that tells us about Russian intentions, and what we should expect in 2018 and 2020. I'm deeply concerned that if we do not work in lockstep with the states to secure our elections, we could be here in two or four years talking about a much worse crisis.
The hearing will feature two panels.
First panel will include expert witnesses from DHS and FBI to discuss Russian intervention in 2016 elections and U.S. government efforts to mitigate the threat.
The second panel will include witnesses from the Illinois State Board of Elections, the National Association of State Elections and Directors, National Associations of Secretary of States and an expert on election security to give us their on-the-ground perspective on how federal resources might be brought to bear on this very important issue.
For our first panel, I'd like to welcome our witnesses today: Dr. Samuel Liles, acting director of Cyber Division within the Office of Intelligence and Analysis at the Department of Homeland Security; Jennifer (sic) Manfra, acting deputy undersecretary, National Protection and Programs Dictorate (sic), also at DHS.
And Jeanette, I think I told you next time you came I did not want "acting" in front of your name. So now I've

publicly said that to everybody at DHS. Hopefully next time that will be removed.
And Bill Priestap. Bill's the assistant director for Counterintelligence Division at the Federal Bureau of Investigation.
Bill, I want to thank you for the help that you have personally provided to the investigative staff of this committee, as we've worked through, so far, over five and a half months of our investigation into the 2016 elections.
As you're well aware, this committee is in the midst of a comprehensive investigation on the specific issue: the extent to which Russian government under the direction of President Putin conducted intelligence activities, also known as Russian active measures, targeted at the 2016 U.S. elections. The intelligence community assesses that, while Russian influence obtained and maintained access to elements of multiple U.S. state and local election boards, those systems were not involved in vote tallying.
During the first panel, I would like to address the depth and the breadth of Russian government cyber activities during the 2016 election cycle, the efforts of the U.S. government to defend against these intrusions, and the steps that DHS and FBI are taking to preserve the foundation of our democracy's free and fair elections in 2018 and beyond.
I thank all three of our first witnesses.
I turn to the vice-chairman.
WARNER: Thank you, Mr. Chairman.
And welcome to the witnesses.
And, Bill, thank you again for all the work you've done with us.
WARNER: We all know that in January, the entire intelligence community reached the unanimous conclusion that Russia took extraordinary steps to intervene in our 2016 presidential elections. Russia's interference in our elections in 2016 I believe was a watershed moment in our political history.
This was one of the most significant events I think any of us on this dais will be asked to address in our time as senators. And only with a robust and comprehensive response will we be able to protect our democratic processes from even more dramatic incursions in the future.
Much of what the Russians did at this point, I think at least in this room, is -- was well known: spreading fake news, flooding social media, hacking personal e-mails and leaking them for maximum political benefit.
Without firing a shot and at minimal cost, Russia sowed chaos in our political system and undermined faith in our democratic process. And as we've heard from earlier witnesses, sometimes that was aided by certain candidates, in terms of their comments about the legitimacy of our democratic processes.
Less well understood, though, is the intelligence community's conclusion that they also secured and maintained access to elements of multiple U.S. state and local electoral boards.
Now, again, as the chairman has said, there's no reason to doubt the validity of the vote totals in the 2016 election. However, DHS and the FBI have confirmed -- and I'm going to come back to this repeatedly -- only two intrusions into the voter registration databases, in both Arizona and Illinois, even though no data was modified or deleted in those two states.
At the same time, we've seen published reports that literally dozens -- I've seen one published report that actually said 39 states -- were potentially attacked.
Certainly is good news that the attempts in 2016 did not change the results of that election. But the bad news is this will not be their last attempt. And I'm deeply concerned about the danger posed by future interference in our elections and attempts by Russian to undermine confidence in our whole electoral system.
We saw Russian -- we saw recently -- and this was just not happening here, obviously -- we saw recently Russian attempts to interfere in the elections in France. And I thank the chairman that next week we'll be having a hearing on some of these Russian efforts in Europe.
We can be sure that Russian hackers and trolls will continue to refine their tactics in the future -- future,

especially if there's no penalty for these malicious attacks.
That's again, one reason I think that the Senate voted so overwhelmingly last week, and I thank all my colleagues for that 97-2 vote to strengthen our sanctions on Russia. I hope that that action sends a strong message to Mr. Putin that there will be a heavy price to pay for attacks against the fundamental core of our democratic system.
Make no mistake, it's likely that we'll see more of these attacks not just in America but against our partners. I heard this morning coming on the radio that the Russians are already actively engaged in the German election cycle, which takes place this fall.
Now, some might say, "Well, why -- why the urgency?"
I can assure you, you know, we have elections in 2018, but in my home state of Virginia, we have statewide elections this year. So this needs a sense of urgency.
The American electoral election process, the machinery, the Election Day manpower, the actual counting and reporting primarily is a local and state responsibility. And in many states, including my own, we have a very decentralized approach, which can be both a strength and a weakness.
WARNER: In Virginia, for instance, decentralization helps deter large-scale hacking or manipulation, because our system is so diffuse. But Virginia localities use more than a dozen different types of voting machines, none of which are connected to the internet while in use, but we have a number of machine-read -- machine -- reader (ph) machines, so that they -- the tabulations actually could be broken into on an individual machine basis.
All this makes large cyber-attacks on electoral system, because of the diffusion, more difficult. But it also makes maintaining consistent, coordinated cyber defenses more challenging as well.
Furthermore, states may be vulnerable when it comes to the defense of voter registration and voter history databases. That's why I strongly believe that that the threat requires us to harden our cyber defenses and to thoroughly educate the American public about the danger.
Yesterday, I wrote to the secretary of homeland security. I urged DHS to work closely with state and local election officials to disclose publicly -- and I emphasize publicly -- which states were targeted. Not to embarrass any states, but how can we put the American public on notice when we've only revealed two states, yet we have public reports that there are literally dozens? That makes absolutely no sense.
I know it is the position of DHS that since the states were victims, it is their responsibility. But I cannot believe that this was an attack on physical infrastructure in a variety of states, there wouldn't be a more coordinated response.
We are not making our country safer if we don't make sure that all Americans realize the breadth and the extent of what the Russians did in 2016, and, frankly, if we don't get our act together, what they will do in an -- a even more dramatic form in 2018 and 2020.
And candidly, the idea of this kind of bureaucratic, "Well, it's not my responsibility, not my job," I don't believe is an acceptable decision.
So, I'm going to hope from our witnesses, particularly our DHS -- DHS witnesses, that we hear a plan on how we can get more information into the bloodstream, how we can make sure that we have better best practices, so that all states are doing what's needed.
I'm not urging or suggesting that in any way the federal government intervenes in what is a local and state responsibility. But to not put all Americans on notice, not -- and to have the number of states that were hacked into or attempt to be hacked into still kept secret is -- is just crazy in my mind.
So, my hope is that we will get some answers. I -- I do want to thank the fact that in January, DHS did designate the nation's electoral infrastructure as critical infrastructure. That's important. But if we call it critical infrastructure but then don't tell the public how many states were attacked or potentially how many could be attacked in the next cycle, I don't think we get to where we need to be.
So, we're going to have -- see more of this. This is the new normal. I appreciate the chairman for holding this

hearing. And I'm going to look forward very much to getting my questions answered.
Thank you.
BURR: Thank you, Vice Chairman.
With that, Dr. Liles, I understand you're going to go first. The floor is yours.
LILES: Chairman Burr, Ranking Member Warner and distinguished members of the committee, thank you for the invitation to be here.
My name is Sam Liles. I represent the Cyber Analysis Division of the Department of Homeland Security's Office of Intelligence and Analysis. Our mission is to produce cyber-focussed intelligence, information and analysis, represent our operational partners like the NCCIC to the intelligence community, coordinate and collaborate on I.C. products, and share intelligence and information with our customers at the lowest classification possible.
We are a team of dedicated analysts who take threats to the critical infrastructure of the United States seriously.
I'd like to begin by clarifying and characterizing the threat we observed to the election infrastructure in the 2016 election.
LILES: Prior to the election, we had no indication that adversaries or criminals were planning cyber operations against the U.S. election infrastructure that would change the outcome of the coming U.S. election.
However, throughout spring and early summer 2016, we and other -- others in the I.C. began to find indications that the Russian government was responsible for widely reported compromises and leaks of e-mails from U.S. political figures and institutions.
As awareness of these activities grew, DHS began in 2016 to receive reports of cyber-enabled scanning and probing of election- related infrastructure in some states.
From that point on, I&A began working to gather, analyze and share additional information about the threat. I&A participated in red team events, looking at all possible scenarios, collaborated and co-authored production with other intelligence community members and the National Intelligence Council. We provided direct support to the department's operational cyber center, the National Cyber Security and Communications Integration Center and worked hand-in-hand with the state and local partners to share threat information related to their networks.
By late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors.
It is important to note that none of these systems were in involved in vote tallying. Our understanding of that targeting, augmented by further classified reporting is that's still consistent with the scale and scope.
This activity is best characterized as hackers attempting to use commonly available cyber tools to exploit known system vulnerabilities. This vast majority of the -- the activity we observed was indicative of simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home.
A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in, so to speak.
Finally a small number of the networks were successfully exploited. They made it through the door. Based on activity we observed, DHS made a series of assessments. We started out with, we had no indication prior to the election that adversaries were planning cyber operations against election infrastructure that would change the outcome of the 2016 election. We also assessed that multiple checks and redundancies in U.S. election infrastructures, including diversity of systems, non-internet- connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit and validate the results -- all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected.
We also finally assessed that the types of systems Russian actors targeted or compromised were not involved in vote tallying.
While we continue to evaluate any and all new available information, DHS has not altered any of these prior assessments. Having characterized the threat as we observed it, I'll stop there to allow my NPPD colleague

Jeanette Manfra to talk about more about DHS is working with election systems to add security and resiliency. I look forward to answering your questions.
BURR: Thank you.
Ms. Manfra?
MANFRA: Thank you, sir.
Chairman Burr, Vice Chairman Warner, members of this committee, thank you for today's opportunity to represent the men and women that serve in the Department of Homeland Security.
Today I'm here to discuss the department's mission to reduce and eliminate threats to the nation's critical physical and cyber infrastructure, specifically as it relates to our election.
Our nation's cyber infrastructure is under constant attack. In 2016, we saw cyber operations directed against U.S. election infrastructure and political entities. As awareness of these activities grew, DHS and its partners provided actionable information and capabilities to help -- help election officials identify and mitigate vulnerabilities on their networks.
MANFRA: Actionable information led to detection of potentially malicious activity affecting internet-connected election-related networks, potentially targeted by Russian cyber actors in multiple states. When we became aware of detected activity, we worked with the affected entity to understand if a successful intrusion had in fact occurred.
Many of these detections represented potentially malicious vulnerability scanning activity, not successful intrusion. This activity, in partnership with these potential victims and targets, enhanced our situational awareness of the threat and further informed our engagement with state and local election officials across the country.
Given the vital role that elections have in a free and democratic society, on January 26 of this year, the former secretary of homeland security established election infrastructure as a critical infrastructure sub-sector. As such, DHS is leading federal efforts to partner with state and local election officials, as well as private sector vendors, to formalize the prioritization of voluntary security- related assistance, and to ensure that we have the communications channels and protocols, as Senator Warner discussed, to ensure that election officials receive information in a timely manner and that we understand how to jointly respond to incidents.
Election infrastructure now receives cybersecurity and infrastructure protection assistance similar to what is provided to other critical infrastructure, such as financial institutions and electric utilities. Our election system is run by state and local governments in thousands of jurisdictions across the country. Importantly, state and local officials have already been working individually and collectively to reduce risks and ensure the integrity of their elections. As threat actors become increasingly sophisticated, DHS stands in partnership to support their efforts.
Safeguarding and securing cyberspace is a core mission at DHS. Through out National Cybersecurity and Communications Center, or NCCC, DHS assists state and local customers such as election officials as part of our daily operations. Such assistance is completely voluntary. It does not entail regulation or federal oversight. Our role is limited to support.
In this role, we offer three types of assistance: assessments, information and incident response. For the most part, DHS has offered two kinds of assistance to state and local officials: first, the cyber hygiene service for internet facing systems provides a recurring report identifying vulnerabilities and mitigation recommendations; second, our cybersecurity experts can go on-site to conduct risk and vulnerability assessments and provide recommendations to the owners of those systems for how best to reduce the risk to their networks.
DHS continues to share actionable information on cyber threats and incidents through multiple means. For example, we publish best practices for securing voter registration databases and addressing potential threats to election systems. We share cyber-threat indicators, another analysis that network defenders can use to secure their systems.
We partner with the multistate Information Sharing and Analysis Center to provide threat and vulnerability

information to state and local officials. This organization is partially grant-funded by DHS and has representatives that sit on our NCCC floor and can interact with our analysts and operators on a 24/7 basis. They can also receive information through our field-based personnel stationed throughout the country and in partnership with the FBI.

Finally, we provide incident response assistance at request to help state and local officials identify and remediate any possible cyber incident. In the case of an attempted compromise affecting election infrastructure, we will share that technical information with other states to assist their ability to defend their own systems from similar malicious activity.

Moving forward, we must recognize that the nature of risk facing our election infrastructure will continue to evolve. With the establishment of an election infrastructure sub-sector, DHS is working with stakeholders to establish these appropriate coordinating councils and our mechanisms to engage with them. These will formalize our mechanisms for collaboration and ensures long-term sustainability of this partnership. We will lead the federal effort to support election officials with security and resilience efforts.

MANFRA: Before closing, I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient. It is diverse, subject to local control and has many checks and balances built in. As the risk environment evolves, the department will continue to support state and local partners by providing information and offering assistance.

Thank you very much for the opportunity to testify, and I look forward to any questions.

BURR: Thank you very much.

Mr. Priestap?

PRIESTAP: Good morning.

Chairman Burr, Vice Chairman Warner, and members of the committee, thank you for the opportunity to appear before you today.

My statement for the record has been submitted. And so rather than restating it, I'd like to step back, and provide you a description of the broader threat as I see it. My understanding begins by asking one question. What does Russia want?

As you well know, during the Cold War, the Soviet Union was one of the world's two great powers. However, in the early 1990's, it collapsed and lost power, stature and much territory. In a 2005 speech, Vladimir Putin, referred to this as a major catastrophe. The Soviet Union's collapse left the U.S. as the sole super power. Since then, Russia has substantially rebuilt, but it hasn't been able to fully regain its former status or its former territory. The U.S. is too strong and has too many alliances for Russia to want a military conflict with us. Therefore, hoping to regain its prior stature, Russia has decided to try to weaken us and our allies.

One of the ways Russia has sought to do this is by influence, rather than brute force. Some people refer to Russia's activity, in this regard, as information warfare, because it is information that Russia uses as a weapon. In regards to our most recent presidential election, Russia used information to try to undermine the legitimacy of our election process. Russia sought to do this in a simple manner. They collected information via computer intrusions and via their intelligence officers, and they selectively disseminated e-mails they hoped would disparage certain political figures and shed unflattering light on political processes.

They also pushed fake news and propaganda. And they used online amplifiers to spread the information to as many people as possible. One of their primary goals was to sow discord and undermine a key democratic principle, free and fair elections.

In summary, I greatly appreciate the opportunity to be here today to discuss Russia's election influence efforts. But I hope the American people will keep in mind that Russia's overall aim is to restore its relative power and prestige by eroding democratic values. In other words, its election-related activity wasn't a one-time event. Russia will continue to pose an influence threat.

I look forward to your questions. Thank you.

BURR: Thank you very much to all of our witnesses. For members, we will proceed by seniority for recognition for up to five minutes. And the chairman will tell you when you have used all your time if you proceed that far. Chair would recognize himself for five minutes.
Yes or no to all three of you. Most important question.
BURR: Do you have any evidence that the votes themselves were changed in any way in the 2016 presidential election?
Dr. Liles?
LILES: No, sir. There was no detected change in the vote.
BURR: Ms. Manfra?
MANFRA: No, sir.
BURR: Mr. Priestap?
PRIESTAP: No, sir.
BURR: Bill, to you. This adversary is determined. They're aggressive and they're getting more sophisticated by the day. The diversity of our election system is a strength, but the intrusions in the state systems also show that Moscow is willing to put considerable resources towards an unclear result.
In 2016, we saw voter data stolen. How could Moscow potentially use that data?
PRIESTAP: They could use the data in a variety of ways. Unfortunately in this setting, I can't go into all of them. I think -- first of all, I think they took the data to understand what it consisted of; what's there, so that they can effect better understand and plan accordingly.
And when I say "plan accordingly," plan accordingly in regards to possibly impacting future elections and/or targeting of particular individuals, but also by knowing what's there and studying it. They can determine is it something they can manipulate or not, possibly, going forward. And there's a couple of other things that wouldn't be appropriate in this setting as well.
BURR: To any of you, you've heard the vice chairman talk about the frustration of publicly talking about how many states. Can you tell the American people why you can't disclose which states and the numbers?
I'll turn to Ms. Manfra first.
MANFRA: Thank you for the question, sir. There are -- through the long history that the department has in working with the private sector and state and local on critical infrastructure and cybersecurity issues, we believe it is important to protect the confidentiality that we have and the trust that we have with that community. So when the entity is a victim of a cyber incident, we believe very strongly in protecting the information around that victim.
That being said, what we can do is take the technical information that we learn from the engagement with that victim and anonymize it so it is not identified as to what that entity or individual is. We can take all the technical information and turn that around and share that broadly with -- whether it's the affected sector or broadly across, you know, the entire country. And we have multiple mechanisms for sharing that.
We believe that this has been a very important key to our success in developing trusted relationships across all of these 16 critical infrastructure sectors.
BURR: Are we prepared today to say publicly how many states were targeted?
MANFRA: We, as of right now, we have evidence of 21 states -- election-related systems in 21 states that were targeted.
BURR: But in no case were actual vote tallies altered in any way, shape or form?
MANFRA: That is correct.
BURR: How did the -- how did the French respond to the Russian involvement in the French elections a month ago? Is that something we followed?
Bill?
PRIESTAP: Senator, from the bureau's standpoint, it's something we followed from afar. We did have

engagement with French officials, but I'm just not at liberty to go into what those consisted of.
BURR: OK, we've -- we've talked about last year. Russia's intent, their target. Let's talk about next year. Let's talk about the '17 elections in Virginia. Let's talk about the '18 elections, congressional, and -- and -- and gubernatorial elections. What are we doing to prepare ourselves with this November and next November?
Ms. Manfra?
MANFRA: Yes, sir.
As we noted, we are taking this threat very seriously. And part of that is identifying this community's critical infrastructure subsector. That's allowed us to prioritize and formalize the engagement with them.
Similar to the 2016 elections, we are identifying additional resources, prioritizing our engagement with them through information sharing products, identifying in partnership, again, with the state and local community, those communication protocols -- how do we ensure that we can declassify information quickly should we need to, and -- and get it to the individuals that need it.
We're also -- have committed to working with state and local officials on incident response playbooks. So, how do they understand where to engage with us, where do we engage with them, and how do we -- are we able to bring the entire resources of the federal government to bear in helping the state and local officials secure their election systems?
BURR: Great.
Vice Chairman?
WARNER: Thank you for the answer. At 21 -- 21 states is almost half the country. We've seen reports that were even higher. I concur with the chairman that the vote totals were not changed. But can you explain to me how we're made safer by keeping the identity of 19 of those states secret from the public? Since Arizona and Illinois have acknowledged they were -- they were attacked?
LILES: Well, sir, I'd bring it back to the earlier points you made about the future elections. One of the key pieces for us within I&A is our ability to work with our partners because of how our collection mechanisms work, it's built on a high level of trust...
(CROSSTALK) WARNER: And if this was -- if this was water systems or power systems, would it be -- would the public be safer by not knowing that their water system or power system in their respective state was attacked?
MANFRA: Sir, I can -- in -- for other sectors, we apply the same principles. When we do have a victim of an incident in the electric sector, or the water sector, we do keep the name of that entity confidential. Some of these sectors do have breach reporting requirements that -- that requires the victims...
(CROSSTALK)
WARNER: Are -- are all 21 of the states that were attacked, are they aware they were attacked?
MANFRA: All of the system owners within those states are aware of the targeting. Yes, sir.
WARNER: At the state level, you could have local registrars and other local officials that -- that there may have been an attempt to penetrate at the state level. And you may have local registrars in the respective state that would not even know that their state had been the subject of Russian activities?
MANFRA: We are currently working with state election officials to ensure communication between the local and the -- and the state...
(CROSSTALK)
WARNER: But at this moment in time, there may be a number of state, local -- state, local election officials that don't know their state were targeted in 2016. Is that right?
MANFRA: The -- the owners of the systems that were targeted do know that they were targeted...
(CROSSTALK)
WARNER: The owners may know, but because we have a decentralized system, many local elective -- I just -- I...

MANFRA: I -- I cannot...
WARNER: ...fundamentally disagree. I understand the notion of victimization.
MANFRA: Yes, sir.
WARNER: But I do not believe our country is made safer by holding this information back from the American public. I got -- I have no interest in trying to embarrass any state.
WARNER: But, you know, if -- if this -- because we -- we've seen this for too long in cyber. We've seen it in the financial industry, and others, where people simply try to sweep this under the rug, and assume they'll go along their way. When we're talking about -- I go back to Liles' initial comments.
We had no idea -- we had no ability to predict this before hand. We had 21 states that were tapped. We've got two that have come forward. While no election results were changed, we do know there were a number of states, perhaps you'll answer this. How many states did the Russians actually exfiltrate data, such as voter registration lists?
MANFRA: Prefer not to go into those details in this forum, sir. I can tell you that we're tracking 21 states that were targeted...
(CROSSTALK)
WARNER: Do the states that had their data exfiltrated by the Russians -- are they aware of that?
MANFRA: Yes, sir.
WARNER: And is there any coordinated response on how we're going to prevent this going forward?
MANFRA: Yes, sir.
WARNER: How do we make sure, if states are not willing to acknowledge that they had vulnerabilities that they were subject to attack -- again, we're in a brave new world here and I understand your position. I'm not trying to -- I'm very frustrated, but I'm not -- I -- I -- I get this notion.
But I think we need a re-examination of this policy. You know, the designation by former Secretary Johnson as critical infrastructure. What does that change in terms of how our operations are going forward? By that designation in January, I appreciated it, but what does that really mean in practical terms, in terms of assistance or information sharing?
MANFRA: What it means for -- it means three things, sir. The first is a statement that we do recognize that these systems are critical to the functioning of American life, and so that is an important statement. The second is, that it formalizes and the -- and sustains, the department's prioritization of engagement with this community. And the last is, it provides a particular protection for sharing of information, in particular, with vendors within the election community. That allows us to have conversations to discuss vulnerabilities with potential systems, that we would not have to disclose.
WARNER: I -- I talked to Secretary Kelly last week, and I hope you'll take this -- at least this Senator's message, back to him. I would like us to get more information. What I've heard today is that, there were 21 states, I appreciate that information, but within those 21 states I have no guarantee that local election officials are aware that their state system may have been attacked, number one.
Number two, we don't know how many states actually had exfiltration. And the final question is, have you seen any stoppage of the Russian activities after the election? Or are they continuing to ping and try to feel out our various election systems?
MANFRA: On the first two questions, sir, I will be happy to get back to you. I spoke to the Secretary this morning and look forward to responding to your letter. On the third question, I'll defer to the FBI.
PRIESTAP: Vice Chairman, I just can't comment on our pending investigations related to the cyber...
(CROSSTALK)
WARNER: You can't say whether the -- so, should the public take away a sense of confidence that the Russians have completely stopped, as of November of 2016, trying to interfere or tap into our electoral systems. Is that what you're saying?

PRIESTAP: That's not what I'm saying, sir. I believe the Russians will absolutely continue to try to conduct influence operations in the U.S., which will include cyber intrusions.
WARNER: Thank you, Mr. Chairman.
BURR: Thank you, Vice Chairman.
To DHS and to the Bureau, a quick question, and if you can't answer it, please go back and get us an answer. Would your agency be opposed to the chair and vice chair sending a letter to the 19 states that have not been publicly disclosed, a classified letter, asking them if they would consider publicly disclosing that they were a target of the last election?
PRIESTAP: Sir, I'd be happy to take that question back to my organization, but I would just add that the role your committee is playing in regards to highlighting the Russian' aims and activities, I think, is critically important for this country.
The Bureau is just trying to balance what -- we'll call it the messaging end of that with doing things that hopefully don't impact what we can learn through our investigations. I know it's a fine -- it's a fine balance but -- but the bottom line is you play a key role in raising awareness of that, and I thank you.
BURR: Fair -- fair -- fair concern, and if both of you would just go back and get back with us, we'll proceed from there.
Senator Risch?
RISCH: Thank you much.
So that the American people can have solid confidence in what you've done, and thank you for what you've done, could you give -- could you give the American people an idea -- if you feel the numbers are classified and that sort of thing, you don't have to go into it.
But the number of people that were involved on DHS and the FBI in this investigation -- can you give us a general idea about that? Whichever one of you want to take that question.
Ms. Manfra?
MANFRA: From a DHS perspective, we did amass quite a few resources both from our intelligence and analysis and our operations analysis. To put a number on it is -- is somewhat challenging but, you know...
(CROSSTALK)
RISCH: Would you say it was substantial?
MANFRA: It was a substantial level of effort.
RISCH: You -- you're confident that you got where you wanted to go when you set out to -- to make this investigation?
MANFRA: Yes, sir. One of our key priorities was developing relationships with that community and getting information out, whether it was to specific victims or broader indicators, that we could share.
We accomplished that. We held multiple sessions. We sent over 800 indicators to the community and so we do believe that -- that we accomplished that. We don't want to let that down at all. We want to continue that level of effort and we intend to continue.
RISCH: And I'm focusing on not what you did after you got the information, but how you got the information. You're confident you got what you needed to appropriately advise everyone in this -- what was going on?
MANFRA: Yes, sir. Yes, we did.
RISCH: Mr. Priestap?
PRIESTAP: This -- the FBI considered this a very grave threat and so we dedicated substantial resources to this effort as well. RISCH: OK. Thank you. To both of you, both agencies again, everyone in this committee knows the specificity and identity of the Russian agencies involved. Are you comfortable in identifying them here today, or do you feel -- still feel that's classified?
PRIESTAP: Yeah. Other what was mentioned in the unclassified version of the intelligence community assessment, I'd rather not go into any of those details.

RISCH: And -- and -- were there any of those agencies identified, any of the Russian intelligence agencies, identified in that?
PRIESTAP: It's my understanding that GIU was identified.
RISCH: Homeland Security, same answer?
LILES: Yes, sir.
RISCH: OK. Thank you much. Let me -- let me ask this question and I come at this from a little different perspective, and I think the American people have the right to know this. From all the work that either of your agencies did, all the people involved, all the digging you did through what -- what the Russians had done and their attempts.
RISCH: Did you find any evidence, direct or circumstantial, to any degree, down to a scintilla of evidence, that any U.S. person colluded with, assisted or communicated with the Russians in their efforts?
Mr. Priestap?
PRIESTAP: And sir, I -- I just can't comment on that today. That falls under the special counsel's purview. And I have to defer to him.
RISCH: Are you aware of any such evidence?
PRIESTAP: And I'm sorry, sir, I just can't comment on that.
RISCH: Ms. -- Ms. Manfra?
MANFRA: Sorry, sir. I cannot also comment on that.
RISCH: Thank you.
Thank you, Mr. Chairman.
BURR: Senator Feinstein?
FEINSTEIN: Thanks very much, Mr. Chairman.
Candidly, I'm very disappointed by the testimony. I mean, we have learned a great deal. And the public has learned a great deal. And it seems to me we have to deal with what we've learned.
Mr. Priestap, is that correct? You have said, and I think quite pointedly, that Russia has decided to weaken us through covert influence rather than brute force. And I think that's a correct assessment, and I think you for having the courage to make it.
Here's a question. To the best of the FBI's knowledge, have they conducted covert influence in prior election campaigns in the United States? If so, when, what and how?
PRIESTAP: Yes, absolutely, they've conducted influence operations in the past. What -- what made this one different, in may regards, was of course, the degree, and then with what you can do through electronic systems today.
When they did it in the past, it was doing things like trying to put in biased or -- or half-true stories, get -- getting stories like that into the press or pamphlets that people were -- will -- would read, so on and so forth. The -- the internet is just -- has allowed Russia to do so much more today than they've even been able to do in the past.
FEINSTEIN: So, you're saying prior campaigns were essentially developed to influence one campaign above another, to denigrate a candidate if she was elected and to support another candidate subtly?
PRIESTAP: Yeah, I -- I'm saying that Russia, for years, has conducted influence operations targeting our elections, yes.
FEINSTEIN: Equal to this one?
PRIESTAP: Not equal to this one. No, ma'am.
FEINSTEIN: OK, here we go. What made this one different?
PRIESTAP: Again, I -- I think the -- the scale -- the scale and the aggressiveness of the effort, in my opinion, made this one different. And again, it's -- it's because of the electronic infrastructure, the internet, what have you, today that -- it allowed Russia to do things that in the past they weren't able to do.
FEINSTEIN: Would you say that this effort was tailored to achieve certain goals?

PRIESTAP: Absolutely.
FEINSTEIN: And what would those goals have been?
PRIESTAP: I think the primary goal in my mind was to sow discord and to try to delegitimize our free and fair election process. I also think another of their goals, which the entire United States intelligence community stands behind, was to denigrate Secretary Clinton and to try to help then -- current President, Trump.
FEINSTEIN: Have they done this on -- in prior elections in which they've been involved?
PRIESTAP: Have they...
(CROSSTALK)
FEINSTEIN: Denigrated a specific candidate and or tried to help another candidate?
PRIESTAP: Yes, ma'am, they have.
FEINSTEIN: And which elections were those?
PRIESTAP: Oh -- I'm sorry, I know there -- I -- I'm sorry, I can't think of an example off the top of my head, but even though -- all the way through the Cold War, up to our most recent election -- in my opinion, they have tried to influence all of our elections since then, and this is a common practice.
FEINSTEIN: Have they ever targeted what is admitted here today to be 21 states?
PRIESTAP: If they have, I am not aware of that. That's a -- that scale is different than what I'm aware of what they tried to do in the past. So again, the scale and aggressiveness here, separates this from their previous activity.
FEINSTEIN: Has the FBI looked at how those states were targeted?
PRIESTAP: Absolutely, ma'am.
FEINSTEIN: And what is your finding?
PRIESTAP: We have a number of investigations open in regards to that. In this setting -- I guess, because they're all still pending investigations, I'd rather not go into those details. The other thing I'd ask you to keep in mind is that we continue to learn things. So, there was some activity we were looking at prior to the election. It's not like when the election was finished our investigation stopped. So as we learn more, we share more.
FEINSTEIN: Do you know if it's the intent of the FBI to make this information public at some point?
PRIESTAP: I -- I think this gets back to an -- an issue the vice-chairman raised, and I -- I guess I want to be clear on my position on it. I think it is critically important to raise awareness about Russia's aims to undermine our democracy, and then their tradecraft and how they do it.
My organization -- part of understanding that tradecraft is -- is conducting our investigations where we learn more and more about tradecraft. So we try to balance, what do we need to provide to partners so they can best protect themselves, versus not interrupting our investigations if the information were to made -- be made public.
FEINSTEIN: Thank you very much. PRIESTAP: A balancing act.
FEINSTEIN: My time is up. Thank you.
BURR: Thanks, Senator Feinstein.
The Vice-Chairman and I have already decided that we're going to invite the bureau in for a classified briefing to update all members on the open investigations, and any that we see that might warrant, on their minds, an opening of a -- a new investigation.
In addition, let me remind members that one of the -- one of the mandates of -- of our investigation is that we will, at the end of this, work with bureau and other appropriate agencies to make a public report in as graded public detail as we can, our findings on Russia's involvement in our election.
So, it is the intent of the chair, at least, to make sure that as much as we can declassify, it's done and the public gets a -- a true understanding when we put out a final report.
Senator Rubio?
RUBIO: Thank you, Mr. Chairman.
And that's -- that's critically important. I think the most important thing we're going to do in this report is tell the

American people how this happened, so we're prepared for the next time. And what -- it begins, I think, by outlining what their goals were, what they tried to do, in this regard.
And we know what they tried to do, because they've done it in other countries around the world for an extensive period of time. The first is, undermine the credibility of the electoral process. To be able to say, that's not a real democracy. It's filled with all kinds of problems. The second is, to undermine the credibility of our leaders, including the person who may win.
They want that person to go into office hobbled by scandal and all sorts of questions about them. And the third, ideally, in their minds, I imagine, is to be able to control the outcome in some specific instances. If they think they could, either through public messaging, or even in a worst case scenario by actually being able to manipulate the vote -- which I know has now been repeatedly testified did not happen here.
RUBIO: And, by the way, these are not mutually exclusive. You can do all three, you can only take one. They all work in conjunction. I think you can argue that they have achieved quite a bit, if you think about the amount of time that we have been consumed in this country on this important topic and the political fissures that it's developed.
And the way I always kind of point to it -- and if anyone disagrees I want you to tell me this -- but, you know, we have something in American politics. It's legitimate; both sides do it. It's called opposition research. You find out about your opponent. Hopefully it's embarrassing or disqualifying information if you're the opposition research person. You package it. You leak it to a media outlet. They report it. You run ads on it.
Now imagine being able to do that with the power of a nation state, illegally acquiring things like e-mails and being able to weaponize by leaking -- leaking it to somebody who will post that and create all sorts of noise. I think that's certainly one of the capabilities. The other is just straight-out misinformation, right? The ability to find a site that looks like a real news place, have them run a story that isn't true, have your trolls begin to click on that story. It rises on Facebook as a trending topic. People start to read it. By the time they figure out it isn't true, a lot of people think it is.
I remember seeing one in early fall that President Obama had outlawed the Pledge of Allegiance, and I had people texting me about it. And I knew that wasn't true, but my point is that we have people texting about it, asking if it was. It just tells you -- and I don't know if that was part of that effort, or it was just somebody with too much time on their hands.
And then the third, of course, is the access to our voting systems, and obviously people talk about effecting the tallies. But just think about this -- even the news that a hacker from a foreign government could have potentially gotten into the computer system is enough to create the specter of a losing candidate arguing, the election was rigged. The election was rigged.
And -- and because most Americans, including myself, don't fully understand all the technology that's around voting systems per se. You give that "election is rigged" kind of narrative to a troll and a fake news site, and that stuff starts to spread. And before you know it, you have the specter of a political leader in America being sworn in under the cloud of whether or not the election was stolen because vote tallies were actually changed.
So I don't know why they were probing these different systems, because obviously a lot of the information they were looking at was publicly available. You can buy it -- voter roles. Campaigns do it all the time. But I would speculate that one of the reasons potentially is because, they wanted these stories to be out there. That someone had pinged into these systems creating a specter of being able to argue, at some point, that the election was invalid because hackers had touched election systems in key states.
And that is why I really, truly believe, Mr. Chairman, it is so important that, to the extent possible, that part of it, the systems part, as much of it be available to the public as possible. Because the only way to combat misinformation is with truth and with facts, and explain to people, and I know some of it is proprietary. I know some of it we weren't trying to protect methods and so forth, but it is really critical that people have confidence that when they go vote that vote is going to count and someone's not going to come in electronically and

change it.
And I think they're -- I -- I just really hope we err on the side of disclosure about our systems so that people have full confidence that when they go vote.
Because I can tell you, I was on the ballot in November, and I remember people asking me repeatedly, is my vote going to count? I was almost afraid people wouldn't vote because they thought their vote wouldn't count.
So I just hope as we move forward -- I know that's not your decisions to make in terms of declassifications and the like -- but it is really, really, really important that Americans understand how our voting systems work, what happened, what didn't and that -- be able to communicate that in realtime in the midst of an election.
So that if in 2018 these reports start to emerge about our voting systems being pinged again, people aren't -- we can put out enough information in October and early November so people don't have doubts. And I know that's not your decisions to make, but I just really hope that's part of -- of what we push on here, because I think it's critical for our future.
BURR: Senator Wyden.
WYDEN: Thank you, Mr. Chairman.
Let me say to the three of you, and I say it respectfully, that on the big issue, which is which states were affected by Russian hacking in 2016, the American people don't seem to be getting more information than what they already had before they showed up. We want to be sensitive to security concerns, but that question has to be answered sooner rather than later. I want to send that message in the strongest possible way. We obviously need to know about vulnerabilities, so that we can find solutions, and we need better cybersecurity to protect elections from being hacked in the first place. And that means solutions like Oregon's vote-by-mail system, that has a strong paper trail, error-gapped (ph) computers and enough time to fix the problems if they pop up.
But now to my question: You all mentioned the January intelligence assessment, saying that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying. Your prepared system -- your prepared testimony today makes another point that I think that is important. You say it is likely that cyber-manipulation of U.S. election systems intended to change the outcome of a national election would be detected. So, that is different what we have heard thus far.
So I have two questions for you, Ms. Manfra, and you, Dr. Liles: What level of confidence does the department have in its assessment that 2016 vote tallying was not targeted or compromised? And second, does that assessment apply to state and local elections?
LILES: Thank you, sir, for the question.
So, the level of effort and scale acquired to change the outcome of a national election would make it nearly impossible to avoid detection. This assessment's based on the diversity of systems, the need for physical access to compromise voting machines themselves, the security of pre-election testing employed by the state and local officials. There's a level -- a number of standards and security protocols that are put in place. There's a -- addition, the vast majority of localities engage in logic and accuracy testing, which work to insure voting machines are operating and tabulating as expected.
Before, during, and after the election, there has been an immense amount of media applied to this, which also brings in the idea of people actually watching in and making sure that the election results represent what they see. And plus there's just this statistical anomalies that would be detected, so we have a very high confidence in our assessments.
WYDEN: What about state and local elections? Do you have the same level of confidence?
LILES: So, from the standpoint of a nation-state actor operating against a state and local election system, we would have the same -- for an Internet-connected system, we would have the same level of confidence.
WYDEN: Ms. Manfra?
MANFRA: Yes, sir.
And I think this also gets to Senator Rubio's point about the difficulty in the general public understanding the

variety of systems that are used in our election process.
MANFRA: And so, we broke our level of engagement and concern down a couple of different areas. The voter registration systems, which are often -- can -- usually connected to the internet. We also were looking at the voting machines themselves, which, by best practice and by the voluntary voting standards and guidelines that the Department of Commerce works with the Election Assistance Commission on, is, by best practice -- those are not connected to the internet.
WYDEN: So can Homeland Security assure the public that the Department would be able to detect an attempted attack on vote tallying?
MANFRA: What I would suggest, sir, is that the ability, as has been demonstrated by security researchers, to access remotely, a voting machine to manipulate that vote, and then to be able to scale that across multiple different voting machines made by different vendors, would be virtually impossible to occur in an undetected way within our current election system.
WYDEN: Has the department conducted any kind of post-election forensics on the voting machines that were used in 2016?
MANFRA: We are currently engaged with many vendors of those systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us. We have not conducted...
(CROSSTALK)
WYDEN: So there's no -- there's been no analysis yet?
MANFRA: We have not -- our department has not conducted forensics on specific voting machines.
WYDEN: Do you believe it's important to do that? In terms of being able to reassure Americans that there was no attack on vote tallying?
MANFRA: Sir, I would say that we do currently have voluntary standards in place that vendors are enabled -- and in approximately 35 states, actually require, some level of certification of those voting machines that they are complying with those standards. We would absolutely be interested in working with vendors to conduct that level of analysis.
WYDEN: Let me ask one last question. Obviously, the integrity of elections depends on a lot of people. State and local election officers, equipment vendors, third party contractors.
Are you all, at Homeland Security and the FBI, confident that the federal government has now identified all of the potential government and private sector targets?
MANFRA: Yes, sir. I'm confident that we've identified the potential targets.
WYDEN: OK.
Thank you, Mr. Chairman.
BURR: Senator Collins?
COLLINS: Mr. Priestap, let me start by saying that it's a great pleasure to see you here again. I remember back in 2003, you were detailed to the Homeland Security Committee when I was the chairman and how helpful you were in our drafting the Intelligence Reform and Terrorism Prevention Act. So, thank you for your continued public service.
You testified this morning and answered the question of, what does Russia want? And you said that the Russians want to undermine the legitimacy of our elections and sow the seeds of doubt among the American public.
Despite the exposure and the publicity given to the Russian's efforts in this regard, do you have any doubt at all that the Russians will continue their activities in subsequent elections?
PRIESTAP: I have no doubt. I just can't -- I just don't know the scale on aggressiveness, whether they'll repeat that, if it'll be less or if it'll be more. But I have no doubt they will continue.
COLLINS: Is there any evidence that the Russians have implanted malware or backdoors or other computer techniques to allow them the easier access next time to our election systems?

PRIESTAP: I'm sorry, Senator. I just can't comment on that because of our impending investigations.
COLLINS: Secretary Manfra, the secretaries of state who are responsible for the election systems have a pretty blistering attack on the Department of Homeland Security, in the testimonies that will be given later this morning. And I want to read you part of that and have you respond.
They say, yet nearly six months after the designation -- and they mean the designation of election systems as critical infrastructure -- and in spite of comments by DHS, that they are rushing to establish election protections. No secretary of state is currently authorized to receive classified threat information that would help them to protect their election systems. Why not?
MANFRA: Thank you, ma'am, for that question. I would note that this community -- the secretaries of state, and for those states where they have a state election director, is not one that the department has historically engaged with. And what we have done in the process of building the trust and learning about how they do their work and how we can assist, we have identified the need to provide clearances to that community. And so we have committed to them to work through that process between our department and the FBI.
COLLINS: Let me ask you about your own agency, which is the agency that focuses on critical infrastructure, including our election systems. Now, NPPD is not an official element of the intelligence community that would have routine access to especially sensitive classified information.
So how do you know with any certainty whether you and others in the agency are read into all the relevant classified information that may exist regarding foreign threats to our critical infrastructure, including our election system?
MANFRA: Yes, ma'am. I would say, despite the fact that we're not a part of the intelligence community -- and our focus is on network defense and operations, in partnership with the critical infrastructure and the federal government -- we feel very confident that with the partnership with our own intelligence and analysis division, that serves as an advocate for us within the intelligence community, as well as our direct relationships with many of those individuals in organizations such as the FBI, NSA and others, that we receive information quickly. And when we ask to declassify that, there are responses, and we work through our partners at the intelligence analysis office to ensure that that happens quickly. So is there room for improvement? Absolutely, of course, but we have the full commitment of the intelligence community to support us and get us the information that we need and our stakeholders need.
COLLINS: And, finally, how many states have implemented all the best practices recommended in the document developed by DHS regarding the protection of election systems?
MANFRA: Ma'am, I'd have to get back to you on a specific number of states. I don't have them.
COLLINS: Do you think most states have?
MANFRA: In our informal engagement, many of them noted that they had already adopted some of these and to the extent that they weren't -- they were incorporating them.
COLLINS: I would ask for a response for the record.
MANFRA: Yes, ma'am.
COLLINS: That's a really important point.
BURR: Senator Heinrich?
HEINRICH: Mr. Priestap, I want to thank you for just how seriously you've taken this and how you've answered the questions this morning in your testimony. I think you hit the nail on the head when you said we need to step back and ask the fundamental question, what do the Russians want?
And by outlining that they want to undermine legitimacy in our system, that they want to sow discord, that they want to undermine our free and fair elections, we really have a better lens with which to understand the -- the specifics of what happened in 2016. In -- in your view, were the Russians successful at reaching their goals in their activities in our 2016 elections?
PRIESTAP: I don't know for certain whether the Russians would consider themselves successful. In many

ways, they -- they might argue that because of the time and energy we're spending on this topic, maybe it's distracting us from other things. But, on the other hand, exactly what this committee is doing as far as raising awareness of their activities, their aims, for the American people, to me they've done -- in my opinion, they've done the American public a service in that regard. And so, I guess I don't know but could argue either way.
HEINRICH: Yes. I -- I think the -- the jury's certainly out for the future, but when you look at the amount of discord that was sown and the impact on 2016, I hope that the outcome of what we're doing here is to make sure that in 2018, and in 2020, and 2022, that by no metric will they have been successful.
Mr. Priestap, you stated, very correctly, that one of their primary goals was to delegitimize our democracy. Are -- are you familiar with the term unwitting agent?
PRIESTAP: Yes, I am.
HEINRICH: Can you kind of summarize what that is for us?
PRIESTAP: In an intelligence context, it would be where an intelligence service is trying to advance certain names and they reach out to a variety of people, some of which they might try to convince to do certain things. And the -- the people, person or persons they contact might actually carry those out, but for different reasons than the intelligence service that actually wanted them to carry them out. In other words, they do it unwittingly.
HEINRICH: By effectively reinforcing the Russian narrative and -- and publicly saying that our system is rigged, did then candidate Trump -- now President Trump, become, what intelligence officials call, an unwitting agent?
PRIESTAP: I -- I can't give you a comment on that.
HEINRICH: I -- I don't blame you for not answering that question. We've got about a minute 46 left. Can you talk about the relationship between the election penetration that we saw and the coincident Russian use of, what Senator Rubio very aptly described, of trolls, of bots, of social media, all designed to manipulate the American media cycle and how those two things fit together?
PRIESTAP: I'm sorry. To clarify, fit together the intrusions with the...
(CROSSTALK)
HEINRICH: What's the relationship between what they were doing in our elections, from a technical point of view, and what they were seeking to do in our media cycle, by using trolls, and bots and manipulation to the media cycles.
PRIESTAP: The -- the -- I guess the best way I can describe it is that this was a, my opinion, a well planned, well coordinated, multi-faceted attack on -- on our election process and democracy. And, while that might sound complicated, it was actually really straight forward. They want to collect intelligence from a variety of sources, human and cyber means.
They want to evaluate that intelligence, and then they want to selectively -- they might selectively disseminate some of it. They might use others for more strategic discussions, but at the end of the day, it's all about collecting intelligence that would give them some type of advantage over the United States and/or attempt to influence things. And then, coordinated -- well coordinated, well funded, diverse ways to disseminate things to hopefully influence American opinion.
HEINRICH: This is a very sophisticated, highly resourced...
(CROSSTALK)
PRIESTAP: Absolutely.
HEINRICH: Thank you.
BURR: Senator Blunt?
BLUNT: Thank you. Thank you, Chairman.
Let's talk a little bit about once -- let's start with a comment that DHS made in it's written comment which -- which says, in excess, that the systems Russian actors targeted or compromised were not involved in vote tallying. Now is that because the vote tallying systems are a whole lot harder to get into than the voter registration systems?

MANFRA: I can't make a statement as to why different systems were targeted. What we can assess that is that those vote tallying systems, whether it was the machines or a kiosk that a voter uses at the polling station, or the systems that are used to tally votes, were very difficult to access, and particularly, to access them remotely. And -- and then given the level of observation of -- for vote tallying at every level of the process that adds into, you know, that we would have identified issues there and there were no identified issues. So those two are... (CROSSTALK)

BLUNT: OK. I -- I would think that if you could get into the vote tallying system, and you did want to impact the outcome of an election, obviously, the vote tallying system is the place to do that. And I would also suggest that all of your efforts -- most -- a lot of your efforts should be to continue to do whatever DHS thinks they need to advise. I don't think we should centralize this system to give advice to state and local election officials to be sure that that that vote tallying system is protected at a level above other systems.

You know, the voter registration system is public information. It is generally accessible in lots of ways. It's not nearly as protected, for that reason. You have lots of them put from lots of sources into that system. And I think, Ms. Manfra, you made the point that you said that in a -- the best practice would be to not have the vote tallying system connected in any unnecessary way to the internet. Is that right?

MANFRA: Both the kiosks themselves and vote tallying systems, to not connect them to the internet and to also have, ideally, paper auditing trails as well.

BLUNT: Well, I certainly agree with that. The paper trail is significant and -- and I think more prevalent as people are looking at new systems. But also, I think any kind of third party monitoring, the third -- the first two parties would be the voter and the counting system, just creates another way into the system. So, my advice would be that DHS doesn't want to be in a situation where somehow you're connected to all the voting systems of the country.

And Mr. Liles, I think you said the diversity of our voting system is a great strength of the system. Do you want to comment on that any more?

LILES: Yes, sir. When we were setting it as part of our red teaming activities, we looked at the diversity of the voting system as actually a great strength. And the fact that there were not connected in any one kind of centralized way. So we evaluated that as -- when we were looking at the risk assessment with OCIA, the Office of Cyber Intelligence Analysis -- Infrastructure Analysis, we looked at that as one of the great strengths and our experts at DIC we worked with also said the same thing.

BLUNT: Well, I would hope you'd continue to think about that as one of the great strengths, as you look at this critical infrastructure, because every -- every avenue for federal monitoring is also just one more -- one more avenue for somebody else to figure out how to get into that system.

And again, the voter registration system dramatically different in what it does. All public information accessible, printed out, given to people to use, though you are careful of what information you give and what you don't. But almost all election officials that have this system now, have some way to share that with the public, as a system.

There is no reason to share the security of the vote counting system with the public, or to have it available or accessible. And I would hope that the DHS, or nobody else, decides that you're going to save this system by having more avenues -- more avenues into the system.

MANFRA: Absolutely not, sir. We're fully supportive of the voluntary standards process, and we are engaging with that process with our experts and we continue, again, with the voluntary partnership with the state and local. And we intend to continue that.

BLUNT: Thank you. Thank you, Mr. Chairman.

BURR: Senator King?

KING: Thank you, Mr. Chairman.

Starting with a couple of short questions, Mr. Priestap.

Number one, you've stated this was a very grave threat, that Russia -- the attempts to probe and upset our local election systems. Any doubt it was the Russians?
PRIESTAP: No, sir.
KING: Any doubt that they'll be back?
PRIESTAP: No, sir.
KING: To our DHS witnesses, have the 21 states that you've mentioned, that we know where we had this happen, been notified officially?
MANFRA: Sir, the owners of the systems within those 21 states have been notified.
KING: How about the election officials in those states?
MANFRA: We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states...
(CROSSTALK)
KING: Have you had a conference of all state election officials, secretaries of state here in Washington on this issue?
MANFRA: I have had at least two teleconferences, and in-person conferences -- we will be engaging with them in July, I believe.
KING: Well, I would urge you to put some urgency on this. We've got another election coming in 18 months and if we're talking about systems and registration rules, the time is going by. So, I believe, this is -- as we've already heard characterized, is a very grave threat. It's going to be back and shame on us if we're not prepared.
MANFRA: Yes, sir. We have biweekly -- every other week, we hold a teleconference with all relevant election officials, the national associations that represent those individuals have nominated bipartisan individuals to engage with us on a regular basis.
This is of the utmost urgency for the department and this government to ensure that we have better protections going forward. But the community -- the election community is similarly committed and has been so for years.
KING: And just to be clear, nobody's talking about a federal takeover of local election systems or the federal rules. What we're talking about is technical assistance in information and perhaps some funding, at some point.
MANFRA: Sir, this is similar to our engagement with all critical infrastructure sectors, whether it's the electrical sector, the nuclear sector, the financial sector, is completely voluntary, and it is about this department providing information, both to potential victims, but to all network defenders, to ensure that they have access to what we have access to and can better defend themselves.
KING: Thank you.
Mr. Liles, I'll take issue with something that you said -- that we have a national election and it was just too large, too diverse, to really crack. We don't have a national election. What we have are 50 state elections. And each election in the states can depend upon a certain number of counties.
There are probably 500 people within the sound of my voice who could tell you which ten counties in the United States will determine the next presidential election. And so you really -- a sophisticated actor could hack a presidential election, simply by focusing on particular counties. Senator Rubio, I'm sure, remembers Dade County in the year 2000 and the significance that had to determining who the next president of the United States was.
So, I don't think it works to just say, oh, it's a big system and the very diversity will protect us because it really is county by county, city by city, state by state and a sophisticated actor, which the Russians are, could easily determine where to direct their attack. So I don't want to rely on the diversity.
Second -- a separate point is, what do we recommend? And we've talked about paper backups. The Dutch just had an election where they just decided to make it all paper and count the ballots by hand, for this very reason. So what would you tell my elections clerk in Brunswick, Maine, Ms. Manfra, would be the top three things he or she should think about in protecting themselves in this situation?

MANFRA: Sir, I would say, to first, as previous senators mentioned, prioritize the security of your voting machines and the vote tallying system, ensure that they are not connected to the internet -- even if that is enabled on those particular devices.
Second, ensure that you have an auditing process in place where you can identify anomalies throughout the process, educate polling workers to look for suspicious activity, for example.
KING: But does -- doesn't auditing mean a paper trail, a paper backup?
MANFRA: Yes, sir. I would recommend a paper backup.
KING: And one of the worrisome things, again, on the issue of the national, we talk about how diverse it is, but aren't we seeing a consolidation in terms of the vendors who are producing these machines? MANFRA: Yes, sir. It is my understanding that we are seeing some consolidation in the vendor community. Again, many of them are committed and have engaged on the voluntary voting standards and guidelines, which partly include security.
We will be updating those security guidelines in 2018, and yes, while there is some concern about consolidation, we do look forward to engaging with them, and as of now, they are a very engaged community.
KING: I think this aspect of this question that we're -- this committee is looking at is one of the most important, and frankly, one of the most daunting, because we pretty well determined that they weren't successful in changing tallies and changing votes but they weren't doing what they did, in at least 21 states, for fun.
And they are going to be back, and they're going to be back with knowledge and information that they didn't have before. So I commend you for your attention to this and certainly hope that this is treated with the absolute utmost urgency.
KING: Thank you, Mr. Chairman.
BURR: Senator Lankford?
LANKFORD: Thank you, Mr. Chairman.
Thanks to all of you for being here as well today.
So, Senator King, just as a heads up, there are some states that are like that. For 25 years the Oklahoma election system has had a paper ballot, and an optical scan and it's been a very good back-up for us. We -- we quickly count because of the optical scan, but we're able to go back and verify because of paper.
This is such a big deal and it's such an ongoing conversation that I'm actually in two simultaneous hearings today, I'm running back and forth with. In the Department of Homeland Security, and what we're dealing with with state elections, and with state systems, is also happening in the HSGAC hearing that I'm also at, including my own Oklahoma CIO that's there testifying today, on this same issue.
How we are protecting state systems, state elections and what's happening? I brought this with me today, you all are probably -- this group is very, very familiar with this e-mail. This is the famous e- mail that Billy Rinehart got, from the DNC, while he happened to be on vacation. He was out in Hawaii enjoying some quality time away from his work at the DNC, and he gets a -- an e-mail from Google, it appears, that says someone has used your password, someone just tried to sign-in to your Google account.
Sent it to him and told him someone tried to do it from the Ukraine, and recommended that he go in and change his password immediately. Which, as the New York Times reported, he groggily at 4 a.m., when he saw that e-mail was frustrated by it, went in, clicked on the link, changed his password and went back to bed.
But what he actually did, was just gave the Russian government access to the DNC, and then it took off from there. Multiple other staff members of the DNC got an e-mail that looked just like this. Now, for everyone who has a Google account, will know that really looks like a Google account warning.
It looked like the real thing when you hovered over the changed password, it showed a Google account connection, where it was going to, but it wasn't. It was going to the Russians. About 91 percent, my understanding is, about 91 percent of the hacks that come into different systems, start with a spear phish attack that looks just like this.

So let's -- let's talk about, in practical terms, for our state election folks and what happens in my state and other states. First, for you, Mr. Priestap, how does Russia identify a potential target? Because this is not just a random e-mail that came to him, this was targeted directly at him, to his address. It looked very real, because they knew who he was and where he works. So, how were the Russians that savvy to be able to track this person and how does this work in the future for an election system for a state?
PRIESTAP: So I can't go into great detail in this forum, but I'd say what intelligent services do, not just Russia there, is they're looking for vulnerabilities. That -- that would begin in the cyber sense with computer vulnerabilities. As far as targeting specific individuals, I -- I don't know all the facts surrounding that e-mail and all the e-mails were sent, but my guess is, they didn't just send it to one person. They send it -- sent it the e-mail like that to a whole variety of -- just hoping that one would click on it.
LANKFORD: Right. But how are they getting that information? Are they going to their -- their website, for instance, and gathering all the e-mails for it? I'm trying to figure out, are they tracking individuals to get more information, so they get something that looks like something they would click on?
PRIESTAP: Yes. You hit on it, but a whole variety of ways. They might get it through reviewing open source material, either online or otherwise, but they also collect a lot of information through their -- through human means.
LANKFORD: So, Ms. Manfra, let me ask you this question. When someone, at any location, clicks on a link like this, what access to information do they get typically?
MANFRA: Well, sir, it depends on -- on the system itself. I -- I imagine that's probably a frustrating response, but given the -- and I think this is important for the public to understand, is, as the -- the threat evolves they're going to continue as we educate the public, don't click on certain things. Look at, you know, make sure you know the sender, for instance before you click on it and as our defense gets better the offense is going to look for other means.
And so we look, you know, in this case, ideally, we want people to look and see what -- what is it that they're actually clicking on before they click it. Some organization to -- to say when an individual clicks on that link, they choose to not allow that to go to that destination, because they know it's suspicious or they have some mechanisms in place to put that into a container and look at it. Other organizations don't take those steps and it really depends on your risk management and the technical control that you put in place.
LANKFORD: Let me ask you a quick question. Who has primary responsibility for Federal election integrity? Which agency is the prime mover in that? Obviously, states oversee their own, but which Federal entity is working with the state to say they're the prime person -- or the prime agency to do it? MANFRA: For election cybersecurity, our -- our department, in coordination with the FBI and others, is leading the partnership with state and locals.
LANKFORD: Great. Thank you.
BURR: Senator Manchin?
MANCHIN: Thank you, Mr. Chairman.
And thank all of you for your appearance here today and your testimony. Being a former Secretary of state of the -- my great state of West Virginia, and also being a former governor, my utmost concern was voter fraud. Every time that we would have a report of a fraud, I would see the election participation decrease, the next election cycle, thinking their vote didn't count.
Is there any reason, at all, that any person that has the knowledge that you all have, or anyone that you've -- on our committee here, from the intelligence community, would give you any doubt that Russia was involved, and Russia was very much involved with the intent of doing harm to our election process, as far as the confidence level that voters would have? Do any of you have any concerns, whatsoever, any doubts, that the Russians were behind this and involved in a higher level than ever? All three of you.
PRIESTAP: No -- no doubt from the FBI's end as far as the -- as far as Russia's involvement.

MANCHIN: And you've all interacted with all the intelligence community right?
PRIESTAP: Yes, sir.
MANFRA: Similar, sir. I have no doubt.
MANCHIN : There's not an American right now that should have a reasonable doubt whatsoever that the Russians were involved? Were all 50 states notified on Russia's intentions and activities during the '20 (sic) election cycle? Had you all put an alert out? So if I'd have been secretary of state in charge of my elections in West Virginia, would you have notified me to be on the lookout?
MANFRA: Sir, I can discuss our products that we put out and I'll defer to the FBI on -- on what they put out. We did put out products, not public products, but we did put out products, primarily leveraging our multi-state information sharing analysis center, which has connections to all 50 states CIOs.
And we engaged with the Election Assistance Commission and other national associations that represent those individuals to ensure that we were able to reach, again this was a community that we had not historically engaged with, and so, we relied on those, that we did put out multiple products prior to the election.
MANCHIN: And you're really not sure if these national associations, like (ph) the secretary of states, dispersed that information, put everybody on high alert?
MANFRA: I -- I believe that they did, sir. We also held a conference call, where all 50 secretaries of state, or an election director, if the -- if the secretary of state didn't have that responsibility. In August, and September and again in October, both high level engagement and network defense products.
MANCHIN: And if I could ask this questions to whoever, maybe Mr. Priestap, what was Russia's intention, and do you think they were successful in what they desired to do, even thought they didn't alter -- as you all have said, you can see no alterations of the election results. Do you believe that it had an effect in this election outcome -- in the outcome of this 2016 election?
PRIESTAP: As far as Russia's intention, again, the broader being to undermine democracy and one of the ways they sought to do this, of course, here, was to undermine the legitimacy of our free and fair election.
MANCHIN: Do you believe they were successful in the outcome?
PRIESTAP: No, I -- the FBI doesn't look at that, as far as, did Russia achieve its aims in that regard.
MANCHIN: Let me ask this question. Are there counter actions the U.S. can take to subvert or punish the Russians for what they have done, and their intention to continue? And what's your opinion of the sanctions that we have placed on Russia?
PRIESTAP: Sure. As you know, the FBI doesn't do policy. I'm here today to provide you an overview of the threat picture, at least, as I understand and see it. But obviously the U.S. government did take action post-election in regards to making a number of Russian officials...
(CROSSTALK)
MANCHIN: Have you seen them subside, at all, any of their activities since we have taken some actions?
PRIESTAP: Subside? They have less people to carry out their activities, so it's certainly had an impact on the number of people.
MANCHIN: And finally, with the few seconds I have left, have we shared this with our allies, our European allies, who are going through election processes and have they seen the same intervention in their election process that we have seen from the Russians in ours? PRIESTAP: Sure. I can't speak for DHS, but the FBI is sharing this information with our allies, absolutely.
MANCHIN: How about DHS?
MANFRA: We are also sharing information with our allies.
MANCHIN: Are they seeing a high -- an overaggressive, high activity, from the Russians that they haven't seen at this level before, such as we did during the 2016 election?
LILES: Sir, there is immediate reporting that suggests that. We don't have direct government-to-government relationships from a DHS perspective. There is definitely immediate reporting that they're seeing an increased

activity.
MANCHIN: Thank you.
BURR: Senator Cotton?
COTTON: Thank you all for your appearance today.
Mr. Priestap, in response to Mr. Heinrich's question about whether Donald Trump had become an unwitting agent of Russia, and their efforts to sow discord and discontent about our elections, you said that you decline to answer, which is understandable.
Let's look at this from a different perspective. Since her election defeat, Hillary Clinton has blamed her loss on the Russians, Vladmir Putin, the FBI, Jim Comey, fake news, Wikileaks, Twitter, Facebook and my personal favorite, content farms in Macedonia. In her blaming her loss on these actors, has Hillary Clinton become an unwitting agent of Russian's goals in the United States?
PRIESTAP: And I'm sorry, sir, but I'd rather not comment. It's just something...
(CROSSTALK)
COTTON: I understand. I just wanted to point out that you can look at it from two different...
(CROSSTALK)
PRIESTAP: ...it's just something I haven't given any thoughts to.
COTTON: Let's turn to other matters, then. Would you advise states and localities in the conduct of their elections, or more broadly, in their government services, not to use, or not to do business with Kaspersky Labs, companies that do business with Kaspersky or companies that use Kaspersky products in their systems?
PRIESTAP: Sir, I can't really comment on that in this setting.
COTTON: Miss Manfra, would you advise them not to use Kaspersky products?
MANFRA: I also cannot comment on that in this forum, sir.
COTTON: I don't even have to ask, Dr. Liles. You're reaching for your microphone.
LILES: Yes, sir. I can't comment either.
COTTON: OK. Senator Risch says he'll answer, but I'll let him speak for himself at a later time. Mr. Priestap, we've talked a lot about Russia's intent and activities in our elections but I think it's important that the American people realize that it goes much farther than just elections and the 2016 campaign, as well.
Isn't it true that Russian cyber actors have been probing U.S. critical infrastructure for years?
PRIESTAP: Yes, sir. I can't go into specifics but they probe a lot of things of critical importance to this country.
COTTON: And as the head of counter intelligence, you write in your statement, that quote, "Russia's 2016 presidential election influence effort was its boldest, to date, in the United States" which implies there have been previous efforts. You also say that the FBI had to strengthen the intelligence community assessment because of our history investigating Russia's intelligence operations within the United States. Both of which suggest that this keeps you pretty busy in your portfolio and counterintelligence, is that right?
PRIESTAP: That's correct.
COTTON: And this is -- Russian intelligence threat is not just a cyber threat either. It also is a threat from traditional human intelligence, or what a layman might call spies, is that right?
PRIESTAP: Yes, sir.
COTTON: Do so called diplomats who work down at the Russian embassy in Washington D.C. have a requirement to notify our state department in advance if they plan to travel more than 25 miles, and give that notification 48 hours in advance?
PRIESTAP: They do.
COTTON: And the State Department's supposed to notify the FBI in advance of those travel arrangements, correct?
PRIESTAP: Yes.
COTTON: Is it true that the Russian nationals often fail to give that notification, at all, or they give it at, say, 4:55

on a Friday afternoon before a weekend trip?
PRIESTAP: I'd prefer not to go into those details here, but -- I'll leave it at that. COTTON: Does it complicate you and your agents' efforts to conduct your counterintelligence mission, to have Russian nationals wandering around the country more than 25 miles outside their duty assignment?
PRIESTAP: Sure. If that were to happen, that would absolutely complicate our efforts.
COTTON: The Secretary of Defense recently indicated, at a Armed Services Committee hearing, that Russia is in violation of something called the Open Skies Treaty, a treaty we have with Russia and other nations that allow us to overfly their territory and take pictures and they do the same here. Do we see so called Russian diplomats traveling to places that are in conjunction with open skies flights that Russia's conducting in this country?
PRIESTAP: I'm sorry, I just can't comment on that here.
COTTON: OK. Is it -- so last summer, a American diplomat in Moscow was brutally assaulted on the doorstep of our embassy in Moscow. Did we take any steps to retaliate against Russia for that assault in Moscow? Did we declare persona non grata any of their so called diplomats here in the United States?
PRIESTAP: If I recall correctly, we didn't immediately do anything in that regard.
COTTON: OK. This committee passed, unanimously, in committee last year, something that just passed as part of the (inaudible) in April a provision that would require one, the State Department to notify the FBI of any requests for Russian diplomats to travel outside their embassy and to report violations to you.
It further requires the State Department to report those violations, regularly, to this committee. What's the status of that provision, now that it's been in law for about two months? Is the State Department cooperating more fully with you?
PRIESTAP: I guess I'd rather not comment on that here. We're still working through the implementation of that.
COTTON: Well, I certainly hope they start. Thank you.
BURR: Senator Harris?
HARRIS: Thank you. Ms. Manfra, you mentioned that you notified the owners. I'm not clear on who the owners are. Are they the vendors?
MANFRA: What I meant to clarify is, in some case, it may not be the secretary of state or the state election director who owns that particular system, so in some cases it could be a locality or a vendor.
HARRIS: So is there a policy of who should be notified when you suspect that there's a threat?
MANFRA: We are working through that policy with the secretaries of state, that is one of the commitments that we made to them, as election directors, in order to ensure that they have appropriate information, while preserving the confidentiality of the victim, publicly.
HARRIS: And can you tell us which states - in which states you notified the vendor instead of notifying the secretary of state?
MANFRA: We keep the vendor information confidential as well.
HARRIS: Are there states that you notified where you did not notify the person who was elected, by the people of that state, to oversee elections?
MANFRA: I don't believe that's the case but I will get back to you with a definitive answer.
HARRIS: And how specific was the warning that you sent? What exactly is it that you notified the states or the vendors of?
MANFRA: Depending on the scenario, and the information that we had, and more generally what we do, is when we get classified information, we look to declassify as much as possible to enable...
(CROSSTALK)
HARRIS: Let's talk about the election, yeah.
MANFRA: So for this particular one, what we took was technical information that we had, that we believed was suspicious, and that was emanating from Russia, and was targeting their system, we asked them to look at their

system. We asked, and this was part of the broader dissemination, as well, we asked all states to look at their system, to indentify whether they had an intrusion, or whether they blocked it. In most cases, they blocked it.
HARRIS: Do you have a copy with you of the notification you sent to these various vendors or states?
MANFRA: I do not, ma'am, but we can get back to you.
HARRIS: OK, and will you provide this committee with a copy of the notification you sent to those states or vendors?
MANFRA: Many of them were done in person, but what I can show you is the technical information. That was also rolled up in the information that we published in December, but I can show you what we provided to the states and localities.
HARRIS: And did you notify each of them the same way? Or did you tailor the notification to each state?
MANFRA: We tailor the notification. It's a process for all victim, or potential victim, notification -- us and the FBI, so sometimes it may be an FBI field agent that goes out there, sometimes it may be a department official that goes out there.
HARRIS: OK, so in your follow-up to the committee, please provide us with, specifically, who notified each state, and then who in that state was notified, the vendor or the state election official, and also what specifically they were notified of. I have, in 2007, California worked with leading security researchers, the secretary of state at the time was Deborah Bowen, and they instituted some of the best practices, we believe, for election security. And my understanding is that it is considered a gold standard. So my question is, does DHS have the technical capability and authority to coordinate a study like that for all of the states?
MANFRA: We do have the technical capability and authority to conduct those sorts of studies, ma'am, yes.
HARRIS: Have you pursued that as a viable option to help the states do everything they can to secure their system?
MANFRA: That is one of the areas that we're considering, yes, ma'am.
HARRIS: So have you taken a look at that study that was commissioned in California, in 2007? And if not, I'd encourage that you do.
MANFRA: I have not personally, but I will read it, ma'am.
HARRIS: And I'm also concerned that the federal government does not have all the information it needs in these situations where there's been a breach. Is there any requirement that a state notify the federal government when they suspect there's been a breach?
MANFRA: No, ma'am.
HARRIS: And in terms of the American public and voters in each of these states, can you tell me is there any requirement that the state notify its residents when the state suspects there may be a breach?
MANFRA: I cannot comment. I know that multiple states have different sunshine laws, et cetera, that apply to data breaches within the state, so I couldn't make a general statement about what their requirements are at the state level.
HARRIS: And do any of you have any thoughts about whether there should be such requirements, both in terms of states reporting to the federal government, and also states reporting to their own residents and citizens about any breaches of their election system?
MANFRA: Required data breach reporting is a complicated area. We prefer, and we've had a fair amount of success with, voluntary reporting and partnerships, but we'd be happy to work with your staff in further understanding how that might apply here.
HARRIS: OK, I appreciate that. Any other thoughts, as we think about how we can improve notification and sharing of information? No. OK, thank you.
BURR: Before I move to Senator Reed, let me just say that since a number of members have questioned the agencies, especially those that are here, and the sharing with Congress of the investigation, I'll just say that the Chair and the Vice Chair were briefed at the earliest possible time, and continued to be briefed throughout the

process, and then it was opened up to all the members of the committee. I'm not sure that I had ever shared that with everybody but I just want to make sure that everybody's aware of that.
Senator Reed?
REED: Thanks very much, Mr. Chairman.
Thank you very much, ladies and gentlemen. Let's start with Mr. Priestap. Are you aware of any direction or guidance from President Trump to conduct this investigation about the Russian cruising (ph) in our elections?
PRIESTAP: Sir, I can't comment on that. It could be potentially related to things under the special councils purview.
REED: Thank you.
Ms. Manfra, in terms of home security, are you aware of any direction by the president to conduct these types of operations, or your investigations?
MANFRA: Sir, to clarify the question, direction from the president to...
(CROSSTALK)
REED: The President of the United States has directed that we, the Department of Homeland Security, and other federal agencies conduct a - the activities that you're conducting, essentially investigation, in to Russian hacking in the election.
MANFRA: I can't comment on the president's directions, specifically, but our secretary is committed to understanding what happened, ensuring that we are better protected in the future, so our activities are fully supported.
REED: He has not communicated that this is at the direction of the President of the United States?
MANFRA: No, sir.
REED: Director Liles?
LILES: Sir, this comes directly written down from the IC (ph) who has been working on this for quite a while, and so, and the secretary has completely supported it.
REED: But again, no...
(CROSSTALK)
LILES: Nothing from the president directly, sir.
REED: Thank you. I thought Senator King raised some very interesting issues, in terms of most election - national elections, as much you like to think about it, particularly from Rhode Island, are not decided in certain states, but decided even in certain cities and counties. Which raised an interesting question -- you were very assertive about that you'd be able to diagnose an intrusion that was altering voter -- votes, literally. When could you do that? Within weeks of an election, on Election Day, after Election Day?
LILES: Sir, from an IEC perspective, the way we would do that is by looking at the threats themselves that were targeting specific entities. And the other element that we would look at is, as the reporting itself was coming in, if there was any statistical anomalies we were seeing. And I'd also point out, that we're talking about internet-connected systems here, and not all of the key counties that you would represent would be those internet-connected systems.
REED: But, effectively, like -- I think what you've said is, that you'd really have to wait for confirmation until the results started coming in on election day, which raises the issue of -- even if you detect it on Election Day, what do we do?
The votes have already been cast. Are you -- is anyone planning on -- what's the -- what reaction we take? How do we notify people? What are -- what steps do they take?
LILES: I'd have to defer to other (OFF-MIKE).
MANFRA: Yes, sir. And I do want to clarify, when we say that that activity would be difficult to detect, it would be -- or difficult to go on undetected, it would -- that we're discussing both at the polling station or the jurisdiction -- that it would be hard for somebody to do that without anybody -- not necessarily that the department would --

would have that immediate insight.
And, to answer your question, yes, that is absolutely something that is a part of our planning and -- and what we would look forward to partnering with the state and local officials on understanding.
REED: So we're, again, about 18 months away from election. We have to be able to develop a -- not technical infrastructure, but an organizational infrastructure that could react, maybe on very short notice, to discovery that actual votes were being tampered. Is that accurate?
MANFRA: Absolutely, sir. It is both technical and organizational.
REED: And do you think there's enough emphasis in terms of the resources and support to do that, the collaboration? I -- you've got 50 states, and among those states, many of the voting jurisdictions are not at the state level -- they're the city and town canvasser. Are we taking it serious enough? I guess that's the issue.
MANFRA: Absolutely, sir. This is one of our highest priorities. And I would also note that we're not just looking ahead to 2018, as election officials remind me, routinely, that elections are conducted on a regular basis. And so -- highest priority, sir. Yes.
REED: Let me ask Mr. Priestap, if I've pronounced it incorrectly., forgive me. But you -- you testified today, and your colleagues, that information was exfiltrated by the Russians. What type of information was taken, and what could it be used for?
PRIESTAP: Yes, sir. I don't want to get into the -- the details of which -- what victim information was taken. Again, we've got a variety of pending investigations.
But it -- it -- again, it could be used for a variety of purposes. Could have been taken to understand what's in those systems. It could have been taken to use to try to target -- learn more about individuals, so that they could be targeted.
It could -- it could have been taken in a way to then publicize, just to send a message, that a foreign adversary has the -- ability to take things and to sow doubt in our voters' minds.
REED: Let me ask you this question, as a judgment. Given the activities that the Russians have deployed, significant resources, constant effort over -- as you -- the intelligence community -- probably a decade, do you think they have a better grasp of the vulnerabilities of the American voting system than you have?
PRIESTAP: I hope not. I think it's a -- I think it's an excellent question and I can -- well, first of all, I hope not and I don't think so, but if they did, I don't think they do anymore.
REED: Thank you very much.
BURR: Thank you, Senator Reed.
Before we move to the second panel, one last question, Mr. Priestap, for you.
Is there any evidence that the attempt to penetrate the DNC was for the purposes of launching this election year intrusion process that they went on? Or was this at the time one of multiple fishing expeditions that existed by Russian actors in the United States?
PRIESTAP: In my opinion, it was one of many efforts. You'd call it a fishing expedition, but to determine again, what's out there, what intelligence can they collect. So they don't go after one place. They go after lots of places and then...
BURR: Tens? Hundreds? Thousands?
PRIESTAP: Hundreds. . At least hundreds.
BURR: OK.
I want to wrap up the first panel with just a slight recap.
I think you have thoroughly covered that there's no question that Russia carried out attacks on state election systems. No vote tallies were affected or affected the outcome of the elections. Russia continues to engage in exploitation of the U.S. elections process and elections are now considered a critical infrastructure, which is extremely important and does bring some interesting potential new guidelines that might apply to other areas of critical infrastructure that we have not thought of because of the autonomy of each individual state and the

control within their state of their election systems.
So I'm sure this will be further discussed as the appropriate committees talk about federal jurisdiction, where that extends to. And clearly, I think it's this committee's responsibility as we wrap up our investigation to hand off to that committee somewhat of a road map from what we've learned or areas that we need to address, and we will work very closely with DHS and with the bureau as we do that.
With that, I will dismiss the first panel and call up the second panel.
END

Subject: Intelligence gathering; Committees; Local elections; State elections; Presidential elections; National security; Democracy; Politics;

Location: Russia United States--US

Company / organization: Name: Federal Bureau of Investigation--FBI; NAICS: 922120;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912737473

Document URL: https://search.proquest.com/docview/1912737473?accountid=14026

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Exhibit 32

Report Information from ProQuest

July 12 2017 17:47

Table of contents

S INTEL HEARING ON RUSSIAN INTERFERENCE IN 2016 ELECTION, PANEL 2

Publication info: Political Transcript Wire ; Lanham [Lanham]21 June 2017.
ProQuest document link

Links: Check SFX for Availability

Full text: S Intel Hearing on Russian Interference in 2016 Election, Panel 2
JUNE 21, 2017
SPEAKERS: SEN. RICHARD M. BURR, R-N.C. CHAIRMAN SEN. JIM RISCH, R-IDAHO SEN. MARCO RUBIO, R-FLA. SEN. SUSAN COLLINS, R-MAINE SEN. ROY BLUNT, R-MO. SEN. TOM COTTON, R-ARK. SEN. JAMES LANKFORD, R-OKLA. SEN. JOHN CORNYN, R-TEXAS SEN. MARK WARNER, D-VA. VICE CHAIRMAN SEN. RON WYDEN, D-ORE. SEN. MARTIN HEINRICH, D-N.M. SEN. JOE MANCHIN III, D-W.VA. SEN. KAMALA HARRIS, D-CALIF. SEN. DIANNE FEINSTEIN, D-CALIF.
SEN. ANGUS KING, I-MAINE
WITNESSES: CONNIE LAWSON, INDIANA SECRETARY OF STATE, PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE
MICHAEL HAAS, MIDWEST REGIONAL REPRESENTATIVE, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS
J. ALEX HALDERMAN, PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MICHIGAN
STEVE SANDVOSS, EXECUTIVE DIRECTOR, ILLINOIS STATE BOARD OF ELECTIONS
[*] BURR: I now call the second panel to order, and ask those visitors to please take their seats. As we move into our second panel this morning, our hearing is shifting from a federal government focus to a state-level focus. During this second panel, we'll again -- we'll gain insight into the experiences of the states in 2016, as well as hear about efforts to maintain election security moving forward.
For our second panel, I'd like to welcome our witnesses: the Honorable Connie Lawson, president-elect of the National Association of Secretaries of State and the secretary of state of Indiana; Michael Haas, the Midwest regional representative to the National Association of State Election Directors and the administrator of the Wisconsin Election Commission; Steve Sandvoss, executive director of the Illinois State Board of Elections; and Dr. J. Alex Halderman, professor of computer science and engineering, University of Michigan.
Thank you all for being here.
Collectively, you bring a wealth of knowledge and a depth of understanding of our state election systems, potential vulnerabilities of our voting process and procedures and the mitigation measures we need to take at the state level to protect the foundation of American democracy.
In January of this year, then-Secretary of State -- Secretary of Homeland Security Jeh Johnson designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. DHS stated that the designation of established election infrastructure as a priority within the national infrastructure protection plan.
It enabled the department to prioritize out cybersecurity assistance to state and local election officials for those who requested, it and made it publicly known that the election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer.
Some of your colleagues objected to this designation, seeing it as federal government interference. Today, I'd like to hear your views on this specifically, but more broadly, how the states and the federal government can best work together. I'm a proud defender of states' rights but this could easily be a moment of divided we fall. We must set aside our suspicions and see this for what it is, an opportunity to unite against a common threat.

Together, we can bring considerable resources to bear and keep the election system safe. Again, I'd like to thank our witnesses for being here.
And at this time, I'd turn to the vice chairman for any comments he might make.
The vice chairman doesn't have any.
I will assume, Mr. Haas, that by some process, you have been elected to go first? Unless there is an agreement -- which -- where are we going to start?
HAAS: Actually, I think we were going to defer to Secretary Lawson to start, if that's OK with the chair.
BURR: Madam Secretary, you are recognized.
LAWSON: Well, good morning, Chairman Burr and Vice Chairman Warner and distinguished members of the committee. I want to thank you for the chance to appear before you today. It's an honor to represent the nation's secretaries of state, 40 of whom serve as chief state election officials.
I am Connie Lawson, Indiana secretary of state and I'm also president-elect of the bipartisan National Association of Secretaries of State. I'm here to discuss our capacity to secure state and locally run elections from very significant and persistent nation- state cyber threats.
With statewide elections in New Jersey and Virginia this year and many more contests to follow in '18, I want to assure you and all Americans that election officials across the United States are taking cybersecurity very seriously.
First and foremost, this hearing offers a chance to separate facts from fiction regarding the '16 presidential election. As noted many times, we have seen no evidence that vote casting or counting was subject to manipulation in any state or locality, nor do we have any reason to question the results. Just a quick summary of what we know about documented foreign targeting of state and local election systems. In the 2016 election cycle, as confirmed by the Department of Homeland Security, no major cyber security issues were reported on Election Day, November 8.
Last summer, our intelligence agencies found that up to 20 state networks had been probed by entities essentially rattling the door knobs to check for unlocked doors. Foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois, prompting the FBI to warn state election offices to increase their election security measures for the November election. In more recent days, we've learned from a top-secret NSA report that the identity of a company providing voter registration support services in several states was compromised.
Of course, it's gravely concerning that election officials have only recently learned about the threats outlined in the leaked NSA report, especially given the fact that the formed DHS Secretary Jay Johnson repeatedly told my colleagues and I that no specific or credible threats existed in the fall of '16. It is unclear why our intelligence agencies would withhold timely and specific threat information from election officials.
I have every confidence that other panelists will address voting equipment risk and conceptual attack scenarios for you today. But I want to emphasize some systemic safeguards that we have against cyber attackers.
Our system is complex and decentralized with a great deal of agility and low levels of connectivity. Even within states, much diversity can exist from one locality to the next. This autonomy serves as a check on the capabilities of nefarious actors.
I also want to mention the recent designation of election systems as critical infrastructure. Real issues exist with the designation, including a lack of clear parameters around the order which currently provides DHS and other federal agencies with a large amount of unchecked executive authority over our election's process. At no time between August of '16 and January of '17 did NASS and its members have a thorough discussion with DHS on what the designation means.
Threat sharing had been touted as a key justification for the designation. Yet, nearly six months later, no secretary of State is currently authorized to receive classified threat information from our intelligence agencies. From information gaps to knowledge gaps that aren't being addressed, this process threatens to erode public

confidence in the election process as much as any foreign cyber threat. It's also shredding the rights that states hold to determine their own election procedures subject to the acts of Congress. If the designation ultimately reduces diversity and autonomy in our voting process, the potential for adverse effects from perceived or real cyber effects -- attacks, excuse me -- will likely be much greater and no the other way around. Looking ahead, the National Association -- the NASS Election Security Task Force was created to ensure that state election officials are working together to combat threats and foster effective partnerships with the federal government and other public-private stakeholders. In guarding against cyber threats, the trendline is positive, but more can be done. Most notably, many states and localities are working to replace or upgrade their voting equipment.

If I have one major request for you today, other than rescinding the critical infrastructure designation for elections, it is to help election officials get access to classified information sharing. We need this information to defend state elections from foreign interference and respond to threats.

Thank you. And I look forward to answering your questions.

BURR: Thank you, Secretary Lawson. Who would like to -- Mr. Haas?

HASS: Thank you. Good morning.

Chairman Burr, Vice Chairman Warner and committee members, on behalf of the National Association of State Election Directors, thank you for this opportunity to share what states learned from the 2016 elections and some steps that it will be -- we are taking to further secure our election systems. I serve as Wisconsin's chief election official, and I'm a member of NASS at the executive board.

We do not have a state elected official who oversees elections in Wisconsin. Many of our state election directors across the country are housed in the secretary of state's offices, but some are not.

The 2016 president election reinforced several basic lessons, although sometimes in a new context. For instance, all must understand the importance of constant and effective communication to ensure that all actors have the tools they need. The new twist (ph) in 2016 of course involved communicating about the security of election systems with the Department of Homeland Security as well as the state staff who provide cyber security protection to our voter registration databases.

As we have heard this morning, some states have expressed concerns about the timeliness and the details of communications from Homeland Security regarding potential threats -- security threats to state election systems. The recent reports about attempted attacks on state voter registration systems, which occurred last fall, caught many states by surprise.

We look forward to working with DHS and other federal officials to develop protocols and expectations for communicating similar information going forward. For example, state election officials believe it is important that we be in the loop regarding contacts that DHS has with local election officials regarding security threats such as the spear-fishing attempts that were recently publicized. States should be aware of this information to protect their systems and so that we can provide additional training and guidance to local election officials.

I appreciate the concern that was expressed this morning that this is a two-way street. And we, at the state level, need to also think carefully about how -- how to most effectively communicate with our local election officials if and when there is an incident that we are aware of at the state level. As part of the DHS designation of election systems as critical infrastructure, bodies (ph) such as coordinating counsels can help to facilitate decisions regarding the proper balance between notifying state and local officials, and protecting confidential or sensitive information.

NASED believes that those coordinating bodies should consist of a broad representation of stakeholders. And we have expressed our strong interest to DHS in participating on those bodies. I would also note that the executive board of NASED supports the request of the U.S. Elections Assistance Commission that it serves as the co-sector's specific -- specific agency as the logical federal agency to partner with DHS to provide subject matter expertise and assistance in communicating with local election officials as the EAC has that communication structure already in place.

HASS: The 2016 elections also reinforced the need for constantly enhancing the security of voter registration databases, as we have heard this morning. While hacking into a voter registration system has no effect on tabulating election results, intrusions could result in unauthorized parties gaining access to data, regarding voters, candidates, ballot contests, and polling places.
I would note that while much of that information is public upon request, there may be some confidential data held in those databases, such as the voter's date of birth, the driver's license number, the last four digits of the social security number. Different states have different laws about what pieces of that data is confidential.
The 2016 elections demonstrated that state and local election officials can implement steps to improve the -- the security of voter data, and then (ph) many of these steps are not complicated.
In addition to the cyber hygiene scans and risk assessments, states are implementing greater use of multi-factor authentication, for users of our systems, updating firewalls, the use of white list, to block unauthorized users, and completely blocking access from any foreign IP address.
The final lesson of 2016 I would like to address relates to voting equipment. To be clear, as it has been said many times this morning, there is no evidence that voting machines or election results have been altered in U.S. elections.
I appreciate the committee's emphasis on that. I think that for the public that cannot be states enough, and strongly enough. Still, we as election administrators must exercise vigilance to assure that such theoretical attacks do not become reality, and we must also continue to educate the public about safeguards in the system. Those safeguards include the decentralized structure of elections that we've heard about this morning and the diversity of voting equipment.
Also, in most cases voting equipment is not connected to the Internet, and therefore cannot be attacked through cyber space. Also it is important to keep in mind that 3 out of 4 ballots cast in American elections are on paper ballots. Most ballots cast on touch screen equipment also have a paper trail that voters can immediately verify their votes, and then election officials can use for audits, and recounts.
There are also several redundancies in the testing and certification of voting equipment. It's important to realize that voting equipment is not only used on Election Day. It's functionality is tested several times during the process.
In short, the 2016 election's taught us, that the potential for disrupting election processes in technology, by foreign or domestic actors is a serious and increasing concern. However, we as state election directors, we have had continued cooperation, and more effective communication, along with continued vigilance and innovation, will ensure the integrity of our voting processes and election results.
Again, we look forward to working with our federal partners as we plan for elections going forward. Thank you for the opportunity to share these thoughts and I'd be happy to answer any questions.
BURR: Thank you, Mr. Haas.
Mr. Sandvoss.
SANDVOSS: Good morning. Thank you, Chairman Burr, Vice Chairman Warner, and distinguished members of the committee. As Director of the State Board of Elections, I'd just like to briefly describe what our agency does. We are an independent bipartisan agency created by the 1970 Illinois constitution, charged with general supervision over the election, and registration laws in the state of Illinois.
As all of you seem to be aware, almost a year ago today, on June 23rd, the Illinois State Board of Elections was the victim of a malicious cyber attack of unknown origin, against the Illinois voter registration system database. Because of the initial low volume nature of the attack, the State Board of Election's staff did not become aware of it at first. Almost three weeks later, on July 12th, State Board of Elections IT staff was made aware of performance issues with the IVRS database server. The processor's usage had spiked to 100 percent with no explanation.
Analysis of the server logs revealed that the heavy load was a result of rapidly repeated data base queries on

the application status page of our paperless online voter application website. Additionally, the server log showed the data based queries were malicious in nature. It was a form of cyber attack known as SQL, which is structured query language injection. SQL injections are essentially unauthorized, malicious data base queries entered in to a data field, in a web based application.

We later determined that these SQLs originated from several foreign based IP addresses. SP programmers immediately introduced code changes to eliminate this particular vulnerability in our website. The following day, on July 13th, the SBE IT made the decision to take the website and IVRS database offline to investigate the severity of the attack. SBE staff maintained the ability to log and view all site access attempts.

Malicious traffic from the IP addresses continued, though it was blocked at the firewall level. Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th, when they abruptly ceased. SV staff began working to determine the extent of the breech, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

A week later, on July 19th, we notified the Illinois general assembly of the security breech, in accordance with the Personal Information Protection Act. In addition, we notified the Attorney General's office. On July 21st, the State Board of Election's IT staff completed security enhancements and began to bring the IVRS system back online. A week after that, on July 28th, both the Illinois registration system, and the paperless online voting application became totally functional once again.

Since the attack occurred, the State Board of Elections has maintained the following ongoing activities the DHS scans the State Board of Election's systems for vulnerabilities, on a weekly basis. The Illinois Department of Innovation and Technology, which is a statewide entity that coordinates the IT systems of many of the Illinois state agencies, continuously monitors activity on the Illinois Century Network, which is the general network that provides firewall protection for the state computer systems.

This Department of Innovation and Technology, also called DOIT, provided cyber security awareness training for all state of Illinois employees, ours included. Now the State Board of Election's IT staff continues to monitor web server, and firewall logs on a daily basis. And in addition a virus protection software is downloaded, also on a daily basis. As a result of informing the Illinois Attorney General's office of the breach, the State Board of Elections was contacted by the Federal Bureau Investigation, and we have fully cooperated with the FBI in their ongoing investigation.

The FBI advised that we work with the Department of Homeland Securities, United States Computer Emergency Readiness team, to ensure that there is no ongoing malicious activity on any of the SBE systems. They also confirmed -- that is, the -- the Department of Homeland Security also confirmed that there's no ongoing malicious activity occurring in SBE computer systems.

To comply with the Personal Information Protection Act, nearly 76,000 registered voters were contacted as potential victims of the data breach. The SBE provided information to these individuals on steps to take if they felt that they were the victims of identity theft.

Additionally, the SBE developed an online tool to inform affected individuals of the specific information that was included in their voter record that may have been compromised.

As far as looking to -- for future concerns, one of the concerns facing our state and many others, we believe, is aging voting equipment. The Help America Vote Act established requirements for voting equipment, while -- but while initial funding was made available to replace the old punch-card equipment, additional funding has not been further appropriated.

If additional funding is not available, we would like to receive authorization to use the states' existing HAVA funds to allow spending on enhanced security across all election-related systems. The IVRS database is a federal mandate through the Help America Vote Act.

Cyber attacks targeting end users are also of particular concern. Security training funded and provided by a

federal entity such as the -- the EAC or DHS would also be beneficial, in our view.
In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.
Thank you for the time, and I'm happy to answer any questions.
BURR: Thank you, Mr. Sandvoss.
Dr. Halderman?
HALDERMAN: Chairman Burr, Vice Chairman Warner and members of the committee, thank you for inviting me to speak with you today about the security of U.S. elections.
I'm a professor of computer science, and have spent the last 10 years studying the electronic voting systems that our nation relies on. My conclusion from that work is that our highly computerized election infrastructure is vulnerable to sabotage, and even to cyber attacks that could change votes.
These realities risk making our election results more difficult for the American people to trust. I know America's voting machines are vulnerable, because my colleagues and I have hacked them, repeatedly, as part of a decade of research, studying the technology that operates elections and learning how to make it stronger.
We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case, we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.
As you know, states choose their own voting technology, and while some states are doing well with security, others are alarmingly vulnerable. This puts the entire nation at risk.
In close elections, an attacker can probe the most important swing states or swing counties, find areas with the weakest protection and strike there. In a close election year, changing a few votes in key localities could be enough to tip national results.
The key lesson from 2016 is that these threats are real. We've heard that Russian efforts to target voter registration systems struck 21 states, and we've seen reports detailing efforts to spread an attack from an election technology vendor to local election offices.
Attacking vendors and municipalities could have put Russia in a position to sabotage equipment on Election Day, causing machines or poll books to fail, and causing long lines or disruption. They could have engineered this chaos to have a partisan effect, by striking places that lean heavily towards one candidate.
Some say the fact that voting machines aren't directly connected to the Internet makes them secure, but unfortunately, this is not true. Voting machines are not as distant from the Internet as they may seem.
Before every election, they need to be programmed with races and candidates. That programming is created on a desktop computer, then transferred to voting machines. If Russia infiltrated these election- management computers, it could have spread a vote-stealing attack to vast numbers of machines.
I don't know how far Russia got, or whether they managed to interfere with equipment on Election Day, but there's no doubt that Russia has the technical ability to commit widespread attacks against our voting system, as do other hostile nations. I agree with James Comey when he warned here, two weeks ago, we know they're coming after America, and they'll be back. We must start preparing now.
Fortunately, there's a broad consensus among cybersecurity experts about measures that would make America's election infrastructure much harder to attack. I've co-signed a letter that I ventured into the record from over 100 leading computer scientists, security experts and election officials that recommends three essential steps.
First, we need to upgrade obsolete and vulnerable voting machines, such as paperless touchscreens, and replace them with optical scanners that count paper ballots. This is a technology that 36 states already use. Paper provides a physical record of the vote that simply can't be hacked.
President Trump made this point well on Fox News the morning after -- the morning of the election. He said,

"there's something really nice about the old paper ballot system. You don't worry about hacking."
Second, we need to use the paper to make sure that the computer results are right. This is a common-sense quality control, and it should be routine.
Using what's known as a risk-limiting audit, officials can check a small, random sample of the ballots to quickly and affordably provide high assurance that the election outcome was correct. Only two states, Colorado and New Mexico, currently conduct audits that are robust enough to reliably detect cyber attacks.
Lastly, we need to harden our systems against sabotage and raise the bar for attacks of all sorts by conducting comprehensive threat assessments and applying cybersecurity best practices to the design of voting equipment and the management of elections. These are affordable fixes.
Replacing insecure paperless voting machines nationwide would cost $130 million to $400 million. Running risk-limiting audits nationally for federal elections would cost less than $20 million a year. These amounts are vanishingly small, compared to the national security improvement they buy.
State and local election officials have an extremely difficult job, even without having to worry about cyber attacks by hostile governments. But the federal government can make prudent investments to help them secure elections and uphold voters' confidence. We all want election results that we can trust.
If Congress works closely with the states, we can upgrade our election infrastructure in time for 2018 and 2020. But if we fail to act, I think it's only a matter of time until a major election is disrupted or stolen in a cyber attack.
Thank you for the opportunity to testify today, and for your leadership on this critical matter. I look forward to answering any questions.
BURR: Dr. Halderman, thank you.
The chair would recognize himself for five minutes. Members will be recognized by seniority.
Secretary Lawson, how many states is the secretary of state in charge of the elections process, do you know?
LAWSON: Yes, sir. It's 40. I'm sorry. Yes, sir. It's 40.
BURR: OK. Would you be specific, what do the secretary of states do -- what is it they do not like about elections being designated critical infrastructure?
LAWSON: The most important issue, sir, is that there have been no clear parameters set and even after the three calls that we had with Secretary Jeh Johnson, before the designation was made, we consistently asked for what would be different if the designation was made and how we would communicate. Would it be any different...
(CROSSTALK)
BURR: So nothing has negatively happened except that you don't have the guidance to know what to do?
LAWSON: Nothing has negatively happened to this date, but also, nothing positive has happened.
BURR: Got it. Got it.
Mr. Sandvoss, Illinois is one of the few states that have publicly been identified, I guess that's in part because you took the initiative to do it. You gave a good chronology, 23 June first sign, 12 July state I.T. staff took action, 12 August the attacks stopped.
At what point was the state of Illinois contacted by any federal entity about their system having been attacked or was it the state of Illinois that contacted the federal government?
SANDVOSS: We were contacted by the FBI -- I don't have the exact date but it was after we had referred the matter to the Attorney General's office. My guess would be probably a week after.
BURR: A week after...
(CROSSTALK)
SANDVOSS: After the A.G. was notified by us of this breach.
BURR: And the A.G. was notified approximately when?
SANDVOSS: On July 19th.
BURR: July 19th. OK. At what point did the state of Illinois know that it was the Russians?

SANDVOSS: Actually, to this day, we don't know with certainty that it was the Russians. We've never been told by any official entity. The only one, that we're aware of, that was investigating, was the FBI and they have not told us definitively that it was the Russians. Our I.T. staff was able to identify -- I think it was seven I.P. addresses from a foreign location, I believe it was the Netherlands.
But that doesn't mean that the attack originated in the Netherlands. We have no idea where it originated from.
BURR: Did your I.T. staff have some initial assessments on their own?
SANDVOSS: No, because I think any -- anything of that nature would have been speculative and we didn't want to do that. I think we wanted to leave that to the professional investigators.
BURR: You gave a update on what you're currently doing to enhance the security. DHS weekly security checks. Has the federal -- in your estimation, has the federal government responded appropriately, to date?
SANDVOSS: I believe they have, yes. I've heard nothing from our I.T. division and they'd be the persons that would know. I've heard nothing from them that the DHS's work in that matter has been less than satisfactory.
BURR: Let me ask all of you, except for you, Mr. Sandvoss. Do you believe the extent of cyber threats to election systems should be made public before the next election cycle?
Should we identify those states that were targeted, Mr. Haas?
HAAS: I think as election directors, we're certainly sensitive to the balance that Homeland Security and others need to make. I think so far -- as far as we've gone, we wanted to know, as the victims or potential victims. And then I think as part of the coordinating council and designation of critical infrastructure, there has to be a conversation amongst the election...
(CROSSTALK)
BURR: Is there a right of the public in your state to know?
HAAS: Yes, I believe there is. If there was a hack into our system, I think that our -- we would -- we would certainly want to consult our statutes and so forth, but we would -- we believe in transparency, we would want to let the public know.
BURR: Dr. Halderman?
HALDERMAN: I think the public needs details about these attacks, and about the vulnerabilities of the system, in order to make informed decisions about how we can make the system better and to provide the resources that election officials need. So, yes.
BURR: Secretary Lawson?
LAWSON: I lay awake at night worrying about public confidence in our election systems, and so, I think we need to be very careful and we need to balance the information because the worst thing that we can do is make people think that their vote doesn't count or it could be canceled out.
And so, if telling the public that -- you know, that these attacks are out there and our systems are vulnerable and it doesn't undermine confidence, it makes them know that we are doing everything we possibly can to stop those attacks, I'd be in favor of it.
BURR: I take for granted none of you at the table have evidence that vote tallies were altered in the 2016 election?
HALDERMAN: Correct.
BURR: Dr. Halderman, before I recognize the vice chairman real quickly, when you and your colleagues hacked election systems, did you get caught?
HALDERMAN: We hacked election systems as part of academic research, where we had machines in our facilities...
(CROSSTALK)
BURR: ...I get that. Did you get caught? Did they see your intrusion into their systems?
HALDERMAN: The one instance when I was invited to hack a real voting system, while people were watching, was in Washington D.C. in 2010 and in that instance, it took less than 48 hours for us to change all the votes

and we were not caught.
BURR: Vice chairman?
WARNER: I'd like to thank all the witnesses for their testimony. I find, a little stunning, Mr. Sandvoss, your answer. I don't know -- I think if you saw the preceding panel, you had the DHS and the FBI, unambiguously, say that it was the Russians who hacked into these 21 systems and I find it a little strange that they've not relayed that information to you.
What we discovered in the earlier testimony and that we finally got public disclosure that 21 states were attacked, and under question from -- from Secretary Harris, we found that even though we know those 21 states were attempted to be hacked into, or doors rattled, or whatever analogy you want to use, in many cases, the state election officials, whether the state directors or the secretaries of state, may not even have been notified. I find that stunning. And clearly, lots of local elected officials -- local election officials, where the activities really take place, haven't been notified. So I've got a series of questions and I'd ask for fairly brief responses. Dr. Halderman, can you just again restate, as Senator King mentioned in the earlier testimony, you don't need to disrupt a whole system, you could disrupt a single jurisdiction in a state, and you could, in fact, wipe that ledger clean, you could invalidate potentially not just that local election but then the results at the state -- the congressional level, the states, and ultimately, the nation, is that not correct?
HALDERMAN: Yes, that's correct.
WARNER: So we are not -- while it's important and I believe in our -- the centralized system, we are only as strong as our weakest link. Is that not correct?
HALDERMAN: That's correct.
WARNER: And Mr. Haas, and Secretary Lawson, do you believe that all 21 states that were attacked, that the state election officials are aware?
LAWSON: I can't answer that question, sir. I'm not certain. I will tell you that Indiana has not been notified. I don't know if we're even on the list.
HAAS: I don't know for sure, except that DHS did indicate in a teleconference that all the states that were attacked have been notified.
WARNER: We were told earlier that that's not the case. We were told that they may have been -- the vendors may have been notified. So do you know whether Wisconsin was attacked?
HAAS: We have not been told that -- that we were -- that there was an attack on Wisconsin.
WARNER: Are you comfortable, either one of you, with not having that knowledge?
LAWSON: We are hypersensitive about our security and I would say that when the FBI sent the notice in September, for states to look for certain I.P. addresses to see if their -- their systems had been penetrated, or attempted to be penetrated, we absolutely searched -- in fact, we looked at 15,500,000 log-ins that had happened in our system since the first of January that year.
And so we -- we believe that our system has not been hacked.
HAAS: I would also state that both our office and the chief information officer of the state, and his office, would likely be able to detect that the system was hacked...
(CROSSTALK)
WARNER: Well just, we've got the two leading state election officials not knowing whether their states were one of the 21 that, at least, the Russians probed -- let me finish, please. And you know, I see -- I understand the balance. But the notion that state election officials wouldn't know -- wouldn't know, that local election officials clearly haven't been notified, I appreciate the chairman's offer.
The chairman and I are going to write a letter to all the states. If you view yourself as victims, I think there is a public obligation to disclose. Again, not to re-litigate 2016, but to make sure that we're prepared for 2017, where I have state elections in my state this year, and 2018. And it's -- to do otherwise because there are some -- there are some still in the political process that believe this whole Russian incursion into our elections is a witch

hunt and fake news.
So I could very easily see some local elected officials saying "this is not a problem, this is not a bother. I don't need to tighten up my security procedures at all." And that would do a huge, huge disservice to the very trust, Secretary Lawson, that you say you want to try to present and provide for our voters. So I hope when -- when you receive the letter from our -- and we're going to write this on a confidential basis, but that you would urge your colleagues to come forward, again, not to embarrass any state.
But I find it totally unacceptable, one, that the public doesn't know, that local elected officials -- local election officials don't know that you as two -- as the leaders of the state election officials don't even know whether your states were part of the 21 that has been testified by the DHS that, at least, they were, if not looked at, door jiggled, or actually is the case in Illinois, where actual information from the voter registration efforts were exfiltrated.
So my hope is that you will work with us on a cooperative basis and we want to make sure that the DHS and others are better at sharing at information and you get those classified briefings that you deserve.
BURR: Senator Risch.
RISCH: Thank you very much.
Mr. Sandvoss, I -- July 12th was the date that you first discovered that you had issues. Is that right?
SANDVOSS: Yes, that's correct.
RISCH: And that was a result of a high-volume spike. Is that correct?
SANDVOSS: Yes, that is correct.
RISCH: Then when you looked at it, you found out that the intrusion attempts actually had started June 23rd, is that correct?
SANDVOSS: Yes.
RISCH: So -- and those were low-volume spikes, starting on June 23rd.
SANDVOSS: Yes.
RISCH: All right. So, if they had never cranked up the volume, is it fair to say you would have never discovered it? Or probably wouldn't have discovered it?
SANDVOSS: I would say it would probably not have been discovered -- certainly not right away. And if it was -- the volume was low enough, even an analysis of our server logs might not catch something like that, because it wouldn't stand out.
So I think the answer to your question is yes.
RISCH: Then you said 12 -- or seven days later, the 19th, you notified the attorney general. Is that right?
SANDVOSS: Yes, correct.
RISCH: That was the -- that was the Illinois attorney general, not the U.S. attorney general, is that correct?
SANDVOSS: Yes. State law requires that we notify the attorney general in these instances.
RISCH: So then the next thing that happened is you were contacted by the FBI. Is that correct?
SANDVOSS: Yes.
RISCH: All right. So the question I've got, I'm just -- I'm just trying to get an understanding the facts -- are you assuming that the Illinois A.G. contacted the FBI, or do you know that, or not know that, or (OFF-MIKE).
SANDVOSS: I don't know that for sure, but I -- I would suspect that they probably did, because how else would the FBI know?
RISCH: Right. Well, and that's kind of where I was getting, is that -- that was not the result of some federal analysis -- that there wasn't a federal analysis of this that turned up what had actually happened. Is that -- is that a fair statement?
SANDVOSS: I believe so, yes.
RISCH: You then did some things to try to mitigate what had happened. Had you -- had you shared this with other states, as to what you had done, in order to, I don't know, develop a best practices, if you would?

SANDVOSS: We didn't have any formal notification to all 50 states, no. I think our focus at that time was trying to repair the damage and assess, you know, what needed to be done, especially with respect to the voters who had their, you know, information accessed.
I believe that, once the FBI got -- became aware of this, I know they contacted the different states. I don't believe our attorney general's office did, although I don't know that for certain. But we did not have any formal communication with all 50 states regarding this.
RISCH: And do you believe that you have developed a best- practices action after this attack that you described for us?
SANDVOSS: I believe so, yes.
RISCH: You think it would be appropriate for you to get that out through the secretary of states organization, or other organizations, so that other states could have that.
SANDVOSS: Certainly. Absolutely.
RISCH: OK.
Mr. Halderman, Your hacking that you've described for us -- does -- would your ability -- if you were sitting in Russia right now, wanted to do the same thing that you had done, would that ability be dependent upon the machines, or whatever system is used, being connected to the Internet?
HALDERMAN: That ability would depend on whether pieces of election I.T. equipment -- I.T. offices that are where the election programming is prepared are ever connected to Internet. The machines themselves themselves don't have to be directly connected to the Internet for -- for a remote attacker to target them.
RISCH: So would recommend that -- that the voting system be disconnected from the Internet, that it be a standalone system that can't be accessed from the outside?
HALDERMAN: It's a best practice, certainly, to isolate vote tabulation equipment as much as possible from the Internet, including isolating its -- the systems that are used to program it.
But other peoples of election infrastructure that are critical, such as electronic poll books or online registration systems, do sometimes need to be connected to Internet -- to systems that have Internet access.
RISCH: But that wouldn't necessarily require that it be connected to the Internet for the actual voting process. Is that right?
HALDERMAN: That's right.
RISCH: And then the extrication of that information off of the voting machine -- would that be fair?
HALDERMAN: The -- I think that's fair to say.
RISCH: Thank you.
Mr. Chairman, I think all of this really needs to be drilled down a little bit further, because it seems to me, with this experience, there's probably some really good information where you could put a firewall in place that -- to stop that -- at least minimize it.
Thank you.
BURR: Senator Wyden.
WYDEN: Thank you, Mr. Chairman. And thank -- thank all of you.
I want to start with you, Professor Halderman. What are the dangers of manipulation of voter registration databases, particularly if it isn't apparent until Election Day, when people show up at the polls to vote?
HALDERMAN: I'm concerned that manipulating voter registration databases could be used to try to sabotage the election process on Election Day.
If voters are removed from the registration database, and then they show up on Election Day, that's going to cause -- cause problems. If voters are added to the voter registration database, that could be used to conduct further attacks.
WYDEN: Let me ask, and this can be directed at any of you. I'm trying to get my arms around this role of contractors and subcontractors and vendors who are involved in elections. Any idea, even a ball park number,

of how many of these people there are? Ten, 70, 200?
HALDERMAN: Vendors that host the voter registration system -- I'm sorry, Senator, I don't have a number.
LAWSON: Sir, I don't have an exact number either, but I will -- I will tell you, in Indiana, for an example, we have six different voting system types. Counties make that decision on their own. But they are all certified by our voting system technical oversight program.
WYDEN: That was my main (ph) question.
So somebody is doing certification over these contractors and subcontractors and equipment vendors and the like? Does that include voting machines, by the way? LAWSON: It does. Most states will have a mechanism to certify the voting machines that they're using, the electronic poll books they're using, the tabulation machines that they're using, making sure that they comply with federal and state law, and making sure that they have the audit processes in place.
WYDEN: So you all have a high degree of confidence that these certification processes are not leaving this other world of subcontractors and the like vulnerable?
HALDERMAN: I have several concerns about the certification processes, including that some states do not require certification to federal standards; that the federal standards that we have are unfortunately long overdue for an update and have significant gaps when it comes to security. And that the certification process doesn't necessarily cover all of the actors that are involved in that process, including the day-to-day operations of companies that do pre-election programming.
WYDEN: One last question. We Oregonians and a number of my colleagues are supportive of our efforts to take vote-by-mail national. And we've had it. I was in effect the country's first senator elected by vote-by-mail in 1996. We've got a paper trail. We've got air gap computers. We've got plenty of time to correct voter registration problems if there are any.
Aren't those the key elements of trying to get on top of this? Because it seems to me, particularly the paper trail. If you want to send a message to the people who are putting at risk the integrity of our electoral institutions, having a paper trail is just fundamental to being able to have the backup we need.
I think you're nodding affirmatively, Professor Halderman, so I'm kind of inclined -- or one of you two at the end were nodding affirmatively, and I'll quit while I'm ahead if that was the case -- but would either of you like to take that on?
HALDERMAN: Vote-by-mail has significant cybersecurity benefits. It's very difficult to hack a vote-by-mail system from an office in Moscow. There are -- whether vote-by-mail is appropriate for every state, in every context, is in our system of course a matter for the states, but I think it offers positive security benefits.
WYDEN: All right.
Thank you, Mr. Chairman.
BURR: Senator Blunt?
BLUNT: Dr. Halderman, on that last answer to that last question, how do you count vote-by-mail ballots?
HALDERMAN: Generally, they would be counted using optical scanners.
BLUNT: Exactly. So you count them the same way you count ballots that aren't vote-by-mail in almost every jurisdiction?
HALDERMAN: If the optical scan ballots are subsequently audited, you can get high security from that process, but yes.
BLUNT: Well that's a different -- that's a different question. Your question there is do you prefer paper ballots and an audit trail, and I do too, but let's not assume that the vote-by-mail ballots are counted any differently. They're counted probably at a more central location, but that doesn't mean that all the manipulation you talked about that we need to protect against wouldn't happen in a vote-by- mail election. You've got a way to go back and you've got a paper trail to count.
HALDERMAN: That's correct. There are three things you need: paper, auditing, and otherwise good security

practices.
BLUNT: While I've got you there, on auditing, how would you audit a non-paper system? If it's a touch-screen system, you mentioned Colorado, and New Mexico already did a required sample audit, which I'm certainly not opposed to that if that's what states want to do, or is the best thing to do. How would you do a non-paper audit?
HALDERMAN: Senator, I think it would be difficult or impossible to audit non-paper systems with the technology that we use in the United States, to a high level of assurance.
BLUNT: So even if you -- if you don't have something to audit, it's pretty hard to audit a system that counted -- that didn't leave a trail.
HALDERMAN: It's basically impossible.
BLUNT: So, Mr. Sandvoss, in Illinois, do you certify counting systems?
SANDVOSS: Yes, we do.
BLUNT: And Secretary Lawson, do you certify counting systems?
LAWSON: Yes, sir.
BLUNT: Mr. Haas, in your, your jurisdiction, somebody is certifying those systems that you use?
HAAS: We both rely on the EAC certification and then our commission does a testing protocol and then approves the equipment to be used in the state of Wisconsin.
BLUNT: And back in Illinois, do you then monitor, in any way, that counting system while it's doing the actual counting?
SANDVOSS: No, the actual counting done on Election Day, Election Night, rather, is done locally at the County Clerk's offices or Board of Election Commissioner offices. We certify the voting equipment -- they have to apply for certification and approval, which we conduct a fairly rigorous test of the voting equipment, but then in actual practice, other than -- we do conduct pre-election tests of the voting equipment on a random basis before each election, but there -- it's a limited number of jurisdictions.
BLUNT: And do you do that in a way that allows you, from your central office, to get into the local system? Or do you go to the local jurisdictions or just monitor how they count that -- how they, how they check that counting system?
SANDVOSS: When we do our pre-election tests, we actually visit the jurisdiction.
BLUNT: All right.
Secretary Lawson, similar?
LAWSON: Similar, however, the State does not go into the Counties, but the Counties are required to do a public test, and as I mentioned, it's public. And so they're required to do testing on the machines, the tabulation, there's a bipartisan election board that's there...
(CROSSTALK)
BLUNT: I guess the -- I guess the point I'd want to drive home there is, that not opening that door to the counting system -- if you don't have the door, nobody else can get through that door as well. But there's monitoring, there's local testing, I don't suggest at all that Dr. Halderman's comments aren't important or something we should guard against, it's -- I was an election official for twenty years, including the Chief Election Official for eight of those, and something -- as we were transitioning to these systems -- something I was always concerned about is what could possibly be done that could be done and undetected.
One of the reasons I always liked the audit trail -- that obviously, Dr. Halderman, you do, you do too, is that you do have something to go back -- if you have a reason to go back -- and really determine what happened on Election Day. Let's talk for just a moment about the much more open registration system.
Secretary Lawson, you said you had 15,500 logins. I believe that was -- talk about logging -- what are they logging into, there? The statewide voter registration system that you maintain a copy of?
LAWSON: The 92 County Clerks in Indiana are connected to the statewide voter registration system, and that 15,500,000 logins reflected the work that they did that year.

BLUNT: 15,500,000?
LAWSON: 15,500,000.
BLUNT: So, obviously, that's a system that has lots of people coming in -- in and out of that system all the time. Do local jurisdictions, like if the library does registration, do you have counties where they can also put those registrations directly into the system?
LAWSON: Other than the counties, no sir. But we do have Indianavoters.com, where a voter can go on and register themselves. And it's a record that is compared to the BMV record, and then the counties will find that information in their hopper the next day. And then they will -- or their computer system, and then the next day they will have the ability to determine whether or not the application is correct.
BLUNT: Do all of your jurisdictions, the three jurisdictions here reflected, have some kind of provisional voting, if you get to the voting place on Election Day and your address is wrong, or your name is wrong, or it doesn't occur -- it doesn't appear at all? Do you have a way somebody can cast a ballot before they leave?
LAWSON: Yes, sir.
BLUNT: And in Illinois?
SANDVOSS: Yes, we do.
HAAS: We have provisional ballots, but they are very limited. We are not an NVR -- NVRA state. And we also have Election Day registration, so people can register at the polls.
BLUNT: So, the failure to have your name properly on the -- I understand, Chairman, and I also noticed the time on others. But just -- the registration system is much more open than the tallying system, that doesn't mean the tallying system doesn't need to be further protected. But the registration system, the idea that somebody gets into the registration system -- there are plenty of ways to do that. Unfortunately, we think now other countries and governments may be doing that as well.
BURR: Senator King?
KING: Thank you, Mr. Chairman.
Dr. Halderman, you're pretty good at hacking voting machines, by your testimony. Do you think the Russians are as good as you?
HALDERMAN: The Russians have the resources of a nation-state. I would say their capabilities would significantly exceed mine.
KING: I expected that was going to be your answer, but I wasn't sure whether your modesty would -- but I think that's an important point, because you testified here today that you were able to hack into a voting machine in 48 hours, change the results, and nobody knew you had done it.
And if you could do it, I think the point is, the Russians could do it if they chose. And we've been talking a lot about registrations lists. My understanding is that, quite often, a voter registration list, at some point in the process, is linked up with -- the computer that has the voter registration list, is linked up with configuring the voting machines, and perhaps even tallying votes. Is that true? Can any of you...
(CROSSTALK)
LAWSON: No, sir.
KING: There's -- there's no connection between the registration list and the voting machines?
LAWSON: No.
KING: Illinois? Is that...
(CROSSTALK)
SANDVOSS: Not in Illinois, no.
KING: OK.
HAAS: That's correct. KING: Well, then I was mistaken. Hm?
Yes, Dr. Halderman?
HALDERMAN: I believe that depends on the specific equipment involved. There may be some designs of voting

systems where there -- the sign-in and the vote counting system are linked.
KING: But of course, if, as you testified I think, if the voting registration list is tampered with in some way, on Election Day, it would be chaos. If names disappeared, people arrived at the polls and their names weren't on the list. Isn't that correct, Ms. Lawson?
LAWSON: If a person showed up at the polls to vote and their name wasn't on the list, if they were expecting they would be given a provisional ballot, I think the biggest danger is that the lines at the polls would increase significantly, if there was a large number of folks who had to do that in each precinct.
KING: Right, that was what I was referring to. On August 1st of 2016, press reports have indicated that there was an FBI notification to all of their field offices about the danger of cyber intrusions into voting systems. Supposedly, those were passed on to state election systems. Did you three get something from the FBI around August 1st that gave IP addresses and some warnings about what should be done?
SANDVOSS: Yes, we did receive an FBI flash. It was in August, and you're saying the 1st, I believe that was it.
KING: That was, yeah, I understand that was the date of it.
Ms. Lawson, did you receive that?
LAWSON: Yes, Indiana received a notice from the FBI.
HAAS: We did, as well.
KING: So there is some interconnection. I mean, one of the things that I'm sort of hearing, and I'm frankly appreciative and happy that you all did receive that notice, but there seems to be a lack of information sharing that goes on that we really need to be sure that -- for example, if you learn -- if something happens in Illinois -- some system whereby you can alert your colleagues across the country to look out for this. And if we learn things here in Washington, if the FBI learns things, that they can alert people around the country, because the best time to deal with this is before the election. After the election, or on Election Day, is much more difficult.
Dr. Halderman?
HALDERMAN: Yes, I would support further information sharing.
KING: And then finally, we've talked about what we do about this. Paper trails has come up. Is that the principal defense? Is that -- Dr. Halderman, what if -- I asked the question to the prior panel. What would you tell my elections clerk in Brunswick, Maine, would be the three things most important that they should do, or my secretary of state in Maine, to protect themselves against a threat we know is coming?
HALDERMAN: The most important things are to make sure we have votes recorded on paper, paper ballots, which just cannot be changed in a cyber attack, that we look at enough of that paper in a post- election, risk limiting audit, to know that they haven't -- the electronic records haven't been changed.
And then, to make sure we are generally increasing the level of our cyber security practice. Information sharing is an example of a good and recommended practice, as are firewalling systems and other things that have been suggested.
KING: One final question. Is it possible -- and we -- there are some press reports about this, of a cyber attack on the vendors of these machines, to somehow tamper with the machines before they go out to the states. Is that a risk?
HALDERMAN: I would be concerned about that. And, in fact, the small number of vendors is an example of how our system in practice is not quite as decentralized as it may appear -- that attacks spreading via vendors, or from vendors to their customers, could be a way to reach voting equipment over a very large area.
KING: And there have been press reports that that -- that, in fact, was attempted in 2016.
HALDERMAN: Yes, that's correct.
KING: Thank you, Mr. Chairman. Mr. Chairman, I want to thank you for holding this hearing. This is such important information for the public, and for our democracy. I appreciate your work here.
BURR: Thank you, Senator.
Senator Harris?

HARRIS: Thank you. So there's a saying that I'm sure many of you have heard, which is the -- you know the difference between being hacked and not being hacked, is knowing you've been hacked. And so I appreciate, Dr. Halderman, the recommendations that you and your colleagues have made, because it also seems to cover the various elements of what we need to do to protect ourselves as a country in terms of our elections, which is prevention, and then there's the issue of detection and also resilience.
Once we -- if we discover that we've been manipulated, let's have the ability to stand back up as quickly as possible. So I have a few questions in that regard. First of all, have each of you -- you received the -- for the states -- received a notification from the FBI? Is that correct?
LAWSON: Yes, ma'am. HAAS: Yes, yes.
SANDVOSS: Yes.
HARRIS: And were any of you also notified by DHS?
Mr. Sandvoss?
SANDVOSS: We had communications with DHS, I don't recall how they were initiated. But I do know that there have been some -- the conference calls with them, and it may have been through the FBI that that occurred.
HARRIS: And I'm speaking of before the 2016 election.
SANDVOSS: Yes.
HARRIS: Yeah.
SANDVOSS: Yes.
HARRIS: Secretary Lawson?
LAWSON: Yes, we had -- we did have conversations with Department of Homeland Security. However, it was through our national association, it was not a direct contact with the state.
HARRIS: Thank you.
HAAS: We were one of the states that took up DHS on their offers to do the cyber hijinks scan. We did have a number of communications with, I believe, a point person in their Chicago office. The FBI alert I think was about a specific incident, but our communications with DHS were more about general steps that could be taken to protect our systems.
HARRIS: So, as a follow-up to this hearing, if each of you -- to the extent that you can recall the nature of those conversations with DHS before the election, if you could share that with the committee, that would be helpful, so we can figure out how notifications might be more helpful to you in the future. If -- hopefully they're not necessary, but if necessary.
Can you, Ms. Lawson, tell me -- Secretary Lawson -- what, in your opinion, are the pros and cons of requiring states to report to the federal government if there's been a breach or a hack? What can you imagine would be the pros and cons of a policy that would require that?
LAWSON: Well, the pro would be that if there -- if, for an example, the FBI or the Department of Homeland Security has better ways to counter those attacks, or to make sure that the reconnaissance is done after such an attack is more sophisticated than the states, then obviously, that would be a pro. Indiana did not take the opportunity to have DHS do our cyber cleaning because we felt that we were in better shape than what they could provide for us, so that would be the con.
HARRIS: OK. And can you, Professor Halderman, tell me -- you know we -- before this last election cycle, there had been a lot of talk through the years, in various states -- Senator Blunt, I'm sure you were part of those discussions about the efficacy of online voting, because it would bring convenience, speed, efficiency, accuracy -- and now we can see that there will be great, potentially, vulnerabilities by doing that. So can you talk with me a little about -- just in terms of policy -- is the day of discussing the need for online voting, has that day passed because of the vulnerabilities that are associated with that?
HALDERMAN: I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would

need in order for voters to have high confidence.
And I say that, having myself done -- hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use.
HARRIS: And isn't that the irony, that the professor of computer engineering -- and I would -- always believed that we need to do more to adopt technology, that government needs to adopt technology -- I think we're advocating good old days of paper voting are the way to go, or at least an emphasis on that, instead of using technology to vote.
Can you tell me also -- any of you, if you know -- it's my understanding that some of the election system vendors have required states to sign agreements that prevent or inhibit independent security testing. Are you familiar with that?
HALDERMAN: That certainly had been something that inhibited attempts by researchers like me to study election systems in the past.
HARRIS: And do you believe that that's a practice that is continuing?
HALDERMAN: I do not -- I don't know the answer to that question.
HARRIS: Have any of you had that experience with any of your vendors?
SANDVOSS: In Illinois, no, we have not. And I don't think Illinois law would allow such an agreement.
LAWSON: I don't believe that would happen in Indiana either, Senator, because in order to sell voting equipment in the state of Indiana, it has to be certified.
HARRIS: Right, which would require testing.
LAWSON: Yes, which requires testing. HARRIS: Thank you, thank you, Mr. Chairman. Thank you.
BURR: Thank you, Senator Harris.
Any Senators seek additional questions or time? Seeing none, let me wrap up. I want to thank all of you for your testimony today.
Secretary Lawson, to you. I really encourage you, as the next representative of secretaries of states, to remain engaged with the federal government, specifically the Department of Homeland Security. And I think with any transition of an administration, there is a handoff and a ramp-up. And I've been extremely impressed with our witness from DHS, who not only was here today, but she has taken the bull by the horns on this issue, and I think you'll see those guidelines very quickly, and I hope that there will be some interaction between secretary of states, since in 40 states you control the voting process.
And you can find the system of federal guidance and collaboration that works comfortably with every secretary of state in your organization. I think it is absolutely critical that we have not only a collaboration, but a communication between the federal government and the states as it relates to our voting systems. If not, I fear that there would be an attempt to, in some way, shape or form, nationalize that.
That is not the answer, and I'll continue to point, Mr. Sandvoss, to Illinois. It is a great example of a state that apparently focused on the IT infrastructure, in staff, and didn't wait for the federal government to knock on the door and say, hey, you got a problem. You identified your problem, you began to remediate it. At some point, the federal government came in as a partner, and I think where we see our greatest strength is to work with states and to chase people like you, Dr. Halderman, who like to break into -- no, I'm just kidding with you. Listen, I think what you did is important.
And I think the questions that you raised about the fact that you really can target to make the impact of what you're trying to do very, very effective. And that's clearly what campaigns do every day. So we shouldn't be surprised if the Russians actually looked at that, or anybody else who wants to intrude into our voting system and our democracy in this country. The -- I've got to admit that the variation of voting methods, six in Indiana, where I don't know how many counties you've got -- I've got 100 counties in North Carolina -- it may be that I find out that every county in North Carolina has the power to determine what voting machines, what voting

software they have.
This can get extremely complicated. Short of trying to standardize everything, which I don't think is the answer, is, how do we create the mechanism for the federal government to collaborate directly with those heads of election systems in the states, and understand up front what we bring to the table, and how we bring it so that we're all looking at the same thing -- the integrity of every vote going to exactly who it was intended to do. So we're going to have debates on paper or electronic, we're going to have debates on what should the federal role be -- at the end of the day, if we haven't got cooperation, and collaboration and communication, I will assure you we will be here with another Congress, with another makeup of the committee, asking the same questions, because we won't have fixed it.
But I think that what Dr. Halderman has said to us is, there are some ways that we can collectively approach this, to where our certainty of intrusions in the future can go down. And the accuracy of the vote totals can be certified. So I thank all the four of you for being here today in our second panel. This hearing is now adjourned.
END

Subject: State elections; Voting machines; Collaboration; National security;

Location: United States--US

Company / organization: Name: National Association of Secretaries of State; NAICS: 813910;

Publication title: Political Transcript Wire; Lanham

Publication year: 2017

Publication date: Jun 21, 2017

Publisher: CQ Roll Call

Place of publication: Lanham

Country of publication: United States

Publication subject: Political Science

Source type: Wire Feeds

Language of publication: English

Document type: News

ProQuest document ID: 1912764930

Document URL: https://search.proquest.com/docview/1912764930?accountid=14026

Last updated: 2017-06-23

Database: Global Newsstream,ABI/INFORM Trade & Industry

Exhibit 33

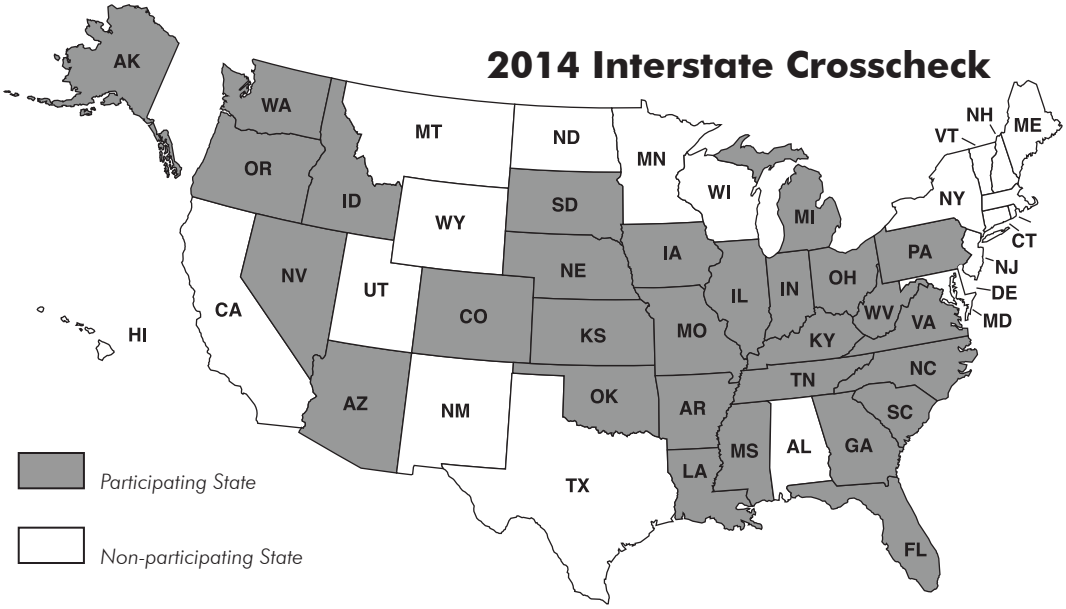
canvassing kansas

AN UPDATE ON ELECTION NEWS FROM THE KANSAS SECRETARY OF STATE'S OFFICE

DECEMBER
2013

Interstate Crosscheck Program Grows

The ninth annual data comparison for the interstate voter registration crosscheck program will be run in January 2014. The program has grown from its original four midwest states (Iowa, Kansas, Missouri and Nebraska) to 29 states in 2014. In 2012 there were 15 participating states and in 2013 there were 22.



The interstate crosscheck program, administered by the Kansas Secretary of State's office, began in December 2005 when the secretaries representing the four original states signed a Memorandum of Understanding to coordinate their offices' efforts in several areas of election administration. Crosschecking voter registration data was one of the areas cited. The first crosscheck was conducted the next year, in 2006.

The program serves two purposes: (1) it identifies possible duplicate registrations among states, and (2) it provides evidence of possible double votes. Most states, including Kansas, process the duplicate registrations by mailing the individuals confirmation notices (as provided in the National Voter Registration Act of 1993) and placing the individuals' names in inactive status. Inactive voters are those for whom election officers have received evidence that they have moved out of the county or state. Once they are given inactive status, their registrations may be canceled if they fail to vote or otherwise contact the election office from the date of the confirmation notice through the second succeeding federal general (November) election.

Cont'd on pg. 6

IN THIS ISSUE

canvassing kansas

Published by the Office of the Secretary of State

EDITORS
Brad Bryant
Kay Curtis

LAYOUT AND DESIGN
Todd Caywood

CONTRIBUTORS
Brad Bryant
Kay Curtis

Suggestions or comments? Please call (785) 368-8095.

Kansas Secretary of State
Memorial Hall
120 SW 10th Ave.
Topeka, KS 66612-1594
(785) 296-4564

From the desk of the Secretary

"Lead, follow, or get out of the way."
Thomas Paine, 1737 - 1809. Kansas has consistently chosen the former when it comes to elections.

In 2005 Kansas took the lead when four states agreed to compare voter registration records with each other annually in order to identify duplicate voter registrations and double votes. Our IT department pulls data from a secure FTP site, runs comparisons and uploads the results to the FTP site on January 15 each year. Then each participating state can download its results and process them according to their own laws and regulations. The Interstate Voter Registration Crosscheck Program had increased to 14 participating states when I took office in 2011.

Convinced of the value of the program, I decided that I would make it one of my highest priorities to increase the number of participating states, hopefully doubling its size. The more states that participate, the more duplicate records each participating state can find. I contacted chief election officers in other states to explain how Crosscheck works and the value of this tool to maintain clean, current, and accurate voter lists to fight voter fraud. As a result, the number of states participating has more than doubled to 29 states that will share voter registration data in January 2014. While I am very pleased that over half of the 50 states are currently on board, I will continue to promote Crosscheck as an effective means of list maintenance.

In 2008 Kansas took the lead in helping voters to find election information when they need it by using internet search engines. As part of the Voting Information Project (VIP), Kansas contracted with ES&S to make programming changes to our ELVIS database so that all states with ES&S can provide a data feed to the VIP program which hosts the data. Google acknowledged our contribution by presenting a Kansas-shaped VIP award to the State of Kansas at the summer NASS conference.

Finally, in 2011 Kansas took the lead as the first state to combine three election-security policies: (1) requiring a government-issued photo ID for voting in person, (2) requiring either a Kansas driver's license number or photocopy of a current photo ID for applying for a mail-in ballot, and (3) requiring a document proving U.S. citizenship when a person registers to vote for the first time. Consequently, Kansas elections are the most secure in the nation against fraud.

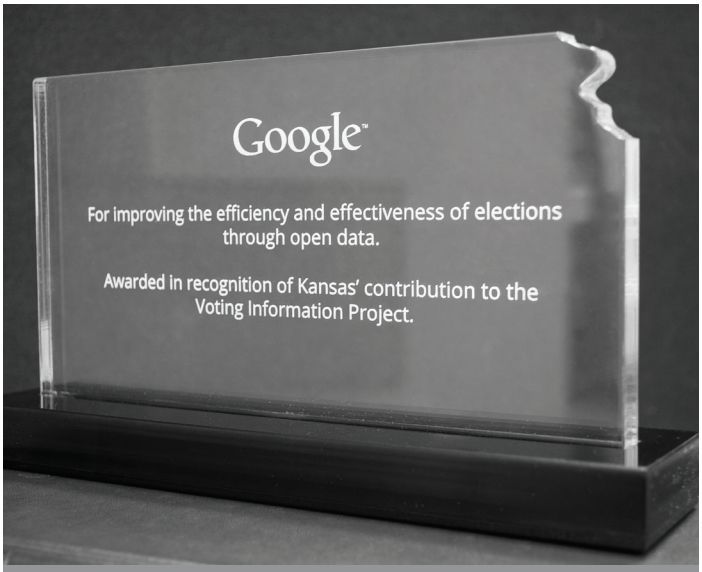
Thank you for all you have done to help implement these reforms. Together we have made Kansas the nation's leader.

Voting Information Project Award Received at NASS

On July 19th, 2013, Google presented an award to recognize Kansas' efforts to improve the efficiency and effectiveness of elections through open data. Eight other states also received the award at the National Association of Secretaries of State 2013 Summer Conference in Anchorage, Alaska. Each of the nine states had participated in the Voting Information Project (VIP) by publishing polling places and other election data as part of the open data effort. Secretary of State Kris Kobach was present to accept the award for his office.

By joining the project on the ground floor, Kansas was among the first states to help registered voters to more readily find election information when they need it and where they are most likely to look for it. Government websites often are not the first place voters look. VIP is similar to the online VoterView feature of the Kansas voter registration system, and voters who perform Google searches for voter registration information will end up at the VoterView website as a result of the VIP.

In the run up to the 2012 general election, 22 million times users queried the Google Civic Information API. According to the VIP program, "When the project started in 2008, nobody involved knew whether the open data effort would have any impact at all. Early adopters took a risk on something new by agreeing to participate and the payoff was immense."



Google award presented to the state of Kansas for its contribution to the Voting Information Project.
Photo by Todd Caywood

The VIP program was initiated as a cooperative effort between the Pew Foundation and Google. As a private charitable organization, Pew's rules do not allow them to pay money to a private for-profit corporation, so Pew asked the Kansas SOS office to serve as a go-between. The SOS office wrote specifications and requested Election Systems & Software to make the required programming changes in the voter registration database. The cost of the programming was paid by Pew to the SOS office and passed on to ES&S. As a result, all states with ES&S databases benefit from the new functionality.

For more information about Kansas participation in the VIP project since 2008, see Canvassing Kansas, September 2010, page 6. ■

Clemens Receives CERA Certification

Crystal Clemens, Seward County Deputy Clerk/Election Officer, completed the Election Center's CERA program this year. Certificates were presented at the Election Center's annual national conference in Savannah, GA, held August 13-17, 2013. Crystal was one of fifty eight election officials to receive the award this year.

CERA (Certified Elections/Registration Administrator) is one of very few nationally recognized programs providing professional training for election administrators. The Election Center itself is a nationwide professional association of local, county and state voter registrars and election administrators that promotes training and best practices, monitors and lobbies on federal legislation, and provides a forum for the exchange of ideas.

Completion of the CERA program requires travel and attendance at a number of training sessions across the country over a period of years. Crystal is one of a small handful of Kansas election officials who have completed it.

Crystal's supervisor, Seward County Clerk Stacia Long, had this to say: "Crystal has always shown great passion for the entire election process. I am very proud of her designation as a CERA. She truly is a great asset to the Election Office and Seward County." ■

Attorney General Issues Opinion on Concealed Carry

The office of Attorney General Derek Schmidt issued a formal opinion on November 27, 2013 in response to questions posed by Secretary of State Kris Kobach. Kobach requested the opinion in a letter dated September 30, 2013, as chief state election officer and on behalf of county election officers across the state.

The issue at the heart of the request was how polling places would be affected by passage of the Personal and Family Protection Act of 2013. The Act, passed as Senate Substitute for House Bill 2052 (2013 Kansas Session Laws, Chapter 105), authorizes persons who possess concealed carry permits to carry weapons into municipal buildings except under specific circumstances. "Municipal building" includes any facility owned or leased by a municipality, which could include facilities used as polling places during advance voting or on election day.

In his letter, Secretary Kobach asked the following questions:

1. ***Does the Act apply to privately-owned facilities used as polling places by verbal agreement?***

2. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when no rent money is paid to the owner or manager of the site?***

3. ***Does the Act apply to privately-owned facilities used as polling places by written agreement when rent money is paid to the owner or manager of the site?***

4. ***If only one room or one portion of a building otherwise not subject to the Act is used as a polling place, does the Act apply to the entire building or only to the area used as a polling place?***

5. ***If an area in a nursing home, assisted living center or long term care facility is used for mobile advance voting pursuant to K.S.A. 25-2812, does the Act apply to the voting area?***

6. ***Do the provisions of the Act applicable to schools still apply to school facilities used as polling places?***

7. ***Is a county government liable for claims of denial of equal protection if various polling places have different levels of security as a result of implementation of the Act?***

At the time of this writing, the secretary of state had just begun to analyze the opinion. The SOS office will communicate further information to CEOs when the analysis is complete. In the meantime, CEOs are encouraged to discuss the opinion with their county attorneys and counselors. The full opinion may be found online: ***http://ksag.washburnlaw.edu/opinions/2013/2013-020.pdf***.

The synopsis from Attorney General Opinion 2013-20 is reproduced here:

Except as described herein, the use of real property as a polling place does not transform the nature of that property for the purposes of the PFPA. Any concealed carry requirements that applied to that property immediately before its temporary use as a polling place continue to apply during its use as a polling place and thereafter.

The Personal and Family Protection Act (PFPA) authorizes concealed carry licensees to carry a concealed handgun into a polling place to the extent that concealed handguns are permitted to be carried into the building in which the polling place is located.

The provisions of K.S.A. 2013 Supp. 75-7c20 apply only to buildings that are owned or leased in their entirety by the state or a municipality. If the PFPA requires concealed carry to be permitted in a state or municipal building, then concealed carry licensees must be permitted to carry a concealed handgun in all parts of the building, including areas used as polling places, with the exception of courtrooms, ancillary courtrooms, and secure areas of correctional facilities, jails and law enforcement agencies.

The governing body or chief administrative officer, if no governing body exists, of a state or municipal building may exempt the building from the provisions of K.S.A. 2013 Supp. 75-7c20 for a set period of time. If a state or municipal building is so exempted, concealed carry may be prohibited by posting the building in accordance with K.S.A. 2013 Supp. 75-7c10.

Cont'd on pg. 6

SOS Office Involved in Litigation

The office of the Kansas Secretary of State finds itself involved in three lawsuits that could affect the voter registration process and the 2014 elections. All are related to the 2011 Kansas SAFE Act. One case deals with the photo ID requirement and the other two deal with the requirement that new voters prove their U.S. citizenship the first time they register to vote.

1. Arthur Sprye and Charles Hamner v. Kris W. Kobach
In a suit filed November 1, 2013, two Osage County voters challenged the constitutionality of the photo ID requirement.

2. Kris W. Kobach, Kansas Secretary of State; and Ken Bennett, Arizona Secretary of State; v. United States Election Assistance Commission
In a suit filed in U.S. District Court in Kansas on August 21, 2013, the Kansas and Arizona Secretaries of State asked for a ruling to require the Election Assistance Commission to include the citizenship requirement in the voter instructions accompanying the universal federal voter registration application form, which is prescribed by the EAC. This lawsuit is in response to the June 17, 2013 ruling by the U.S. Supreme Court in Arizona v. Inter Tribal Council of Arizona regarding the constitutionality of states' requirements that voters provide proof of citizenship. The Court's ruling indicated that states might file suit if the EAC declined to make the necessary changes to the voter registration form administratively.

3. Aaron Belenky, Scott Jones, and Equality Kansas v. Kris Kobach, Kansas Secretary of State, and Brad Bryant, Kansas Elections Director
In a suit filed November 21, 2013, the plaintiffs seek declaratory and injunctive relief to keep the secretary of state's office from implementing a dual voter registration system. The SOS office had developed contingency plans to administer voter registration and ballots to individuals who attempted to register using the universal federal form but who had not provided proof of U.S. citizenship in compliance with Kansas law. No actions have been taken to implement the plan, and no federal elections have occurred in which federal-only ballots were administered to these voters. (See also Canvassing Kansas, September 2013, page 1.)

The goal of the secretary of state's office is to have the cases decided as soon as possible so CEOs and poll workers will know the rules before preparations begin for the 2014 election season. ■

Kobach Reappoints Lehman

Secretary of State Kris Kobach reappointed Tabitha Lehman as Sedgwick County Election Commissioner in September 2013. Her regular term expires on July 19, 2017. This will be Lehman's first full term as election commissioner, having been appointed to fill an unexpired term in 2011.

Lehman was appointed in November 2011 to succeed Bill Gale who resigned his position to pursue other employment. Gale had been appointed in November 2003 to succeed Marilyn Chapman, and he was reappointed in July 2009.

Speaking of her reappointment, Lehman said:
"I appreciate the opportunity to continue serving the voters of Sedgwick County and look forward to providing them with safe and efficient elections in the coming four years." ■

Sedgwick County Election Commissioner Tabitha Lehman
Photo courtesy of Tabitha Lehman

Crosscheck
Cont'd

Evidence of double votes is presented to law enforcement officers for investigation and possible prosecution. The referral is usually made to county law enforcement officers, but state or federal officials may be involved in some cases.

States join the crosscheck by signing a Memorandum of Understanding. The chief state election officer (usually the secretary of state) or a designee may sign the MOU for a given state.

Participating states pull their entire voter registration databases and upload them to a secure FTP site on January 15 each year. The Kansas SOS office IT staff pull the states' data from the FTP site, run the comparison, and upload each state's results to the FTP site. Each state then pulls its results from the FTP site and processes them according to its individual laws, regulations and procedures. In Kansas, results are provided to CEOs with instructions for analyzing them and mailing confirmation notices.

The crosscheck program is one of several list maintenance programs used to keep registration records up to date. (See also Canvassing Kansas, March 2010, page 9.) ■

Attorney General
Cont'd

If the governing body or chief administrative officer of a state or municipal building does not exempt a building from the provisions of K.S.A. 2013 Supp. 75-7c20, then concealed carry licensees must be permitted to carry a concealed handgun inside the building unless adequate security measures are provided and the building is posted as prohibiting concealed carry.

Concealed carry is not required to be permitted in a polling place located inside a privately-owned building unless the county has leased the entire privately-owned building.

Concealed carry is not required to be permitted in polling places located inside public school district buildings because a public school district is not a municipality for the purposes of the PFPA.

An equal protection claim against a county based upon the varying ability of concealed carry licensees to carry a concealed handgun into a polling place would be subject to the rational basis test. ■

Jury List Program Initiated

A 2013 law which went into effect July 1, 2013, requires district courts in Kansas to provide to the secretary of state the names of prospective jurors who indicate on their jury questionnaires that they are not United States citizens. Noncitizens are exempt from jury duty. The secretary of state passes the names on to CEOs for review. If they are found to be registered voters, their registrations are canceled. (See 2013 House Bill 2164; 2013 Kansas Session Laws Chapter 85.)

The relevant section of the law is New Section 1, reproduced below. Most of the bill deals with grand juries.

New Section 1. (a) On and after July 1, 2013, any jury commissioner that receives information regarding citizenship from a prospective juror or court of this state that disqualifies or potentially disqualifies such prospective juror from jury service pursuant to K.S.A. 43-156, and amendments thereto, shall submit such information to the secretary of state in a form and manner approved by the secretary of state. Any such information provided by a jury commissioner to the secretary of state shall be limited to the information regarding citizenship and the full name, current and prior addresses, age and telephone number of the prospective juror, and, if available, the date of birth of the prospective juror. Any such information provided by a jury commissioner to the secretary of state shall be used for the purpose of maintaining voter registrations as required by law.

The secretary of state's office worked with the Office of Judicial Administration (OJA) to design the following procedure to comply with the law:

- The clerk in each of Kansas' 31 judicial districts will submit a monthly report directly to the SOS office containing names of persons who were exempted from jury duty on the basis of their claims to be non-U.S. citizens.
- Reports will be submitted via email on or after the 15th of each month beginning in December 2013.
- The SOS will notify OJA of missing reports. OJA will contact any such district court clerks to remind them to submit their reports.
- If any of the persons listed in the reports are found to be registered voters and their citizenship status is not in doubt, their names will be sent by the SOS office to the appropriate county election officers with instructions regarding the possible cancellation of the persons' voter registration records. ■

State Fair Opinion Poll Results

The Office of the Secretary of State has operated a booth in the Meadowlark Building at the Kansas State Fair in Hutchinson for more than 25 years. The dates of the fair this year were September 6-15. This was the 100th anniversary of the fair, and the theme was "Never Gets Old."

At the booth, the SOS office provides information about agency activities, registers voters, and conducts an opinion poll on current issues. Don Merriman, Saline County Clerk, has assisted the SOS office for many years by lending ES&S iVotronic voting machines to help the fair visitors familiarize themselves with electronic voting technology. We want to recognize and thank Don for his assistance and the Lockwood Company for its donation of ballot programming services.

The SOS booth is mostly staffed by agency employees, but sometimes county election office personnel help out by volunteering to work in the booth. This year's county volunteers were: Sharon Seibel, Ford County Clerk; Debbie Cox, Ford County Deputy Clerk; Donna Maskus, Ellis County Clerk; Don Merriman, Saline County Clerk; Crysta Torson, Lane County Clerk; and Karen Duncan, Lane County Deputy Clerk. Thanks to the volunteers for helping out!

Following are the results of the opinion poll:

Question #1: New Kansas voters must provide proof of citizenship when registering to vote.

709 *I approve of this requirement.*
96 *I do not approve of this requirement.*
27 *I have no opinion about this requirement.*

Question #2: Which university will advance the furthest in the 2014 NCAA Men's Basketball Tournament?

397 *University of Kansas*
196 *Kansas State University*
179 *Wichita State University*
48 *None will make the tournament*

Question #3: Which of these alleged abuses of power by the federal government is the most concerning to you?

342 *NSA secretly collecting phone records of millions of U.S. citizens.*
332 *IRS intentionally discriminating against conservative organizations.*
153 *Presidential political appointees using secret email accounts to conduct official government business.*
132 *White House's sweeping seizure of Associated Press records and cable television documents.*

Question #4: Should the Internal Revenue Service be abolished?

526 *Yes. A flat or fair tax is simpler, cheaper and easier to manage.*
86 *Yes. We shouldn't have to pay income tax anyway.*
125 *No. Better training and oversight will fix most problems.*
2 *No. There is nothing wrong with the IRS.*

Question #5: Who is your favorite super hero?

90 *Xena: Warrior Princess*
379 *Superman*
94 *Wonder Woman*
195 *Batman* ■

Former Longtime Neosho County Clerk Dies

Wayne B. Gibson, Jr., a well known longtime county clerk from Neosho County, died on September 18, 2013, at a hospital in Labette County. Wayne served many years in the Neosho County Clerk's office and was known to Kansas election officials as a hardworking, conscientious public servant.

Gibson started working in the county clerk's office on January 16, 1961 and became Deputy Clerk about a month later. He then became Clerk on July 14, 1971, following the death of his predecessor, Virgil Lowe. Gibson served continuously until his retirement on April 20, 2007. During that time he was elected ten times - in 1972, 1974, 1976, 1980, 1984, 1988, 1992, 1996, 2000 and 2004.

The vacancy created by Gibson's resignation was filled by Randal Neely, who took office on August 1, 2007, and continues in office today. ■

Dominion Seeks Voting System Certification

Dominion Voting Systems, Inc., submitted a letter dated October 4, 2013 requesting certification of its Democracy Suite Version 4.14 voting system. According to Kansas law, a manufacturer seeking certification of its voting system must submit a formal letter, pay a $500 fee, and demonstrate the system at a certification hearing held in Topeka.

A hearing was held at the secretary of state's office on November 21, 2013, attended by Secretary of State Kris Kobach and members of his staff. The Democracy Suite system was demonstrated and explained by Norma Townsend, Don Vopalensky, Jeff Hintz and Michael Kelava. Dominion is represented in Kansas by its subcontractor, Election Source. Dominion also markets and services Premier (formerly Diebold) voting equipment, having purchased Premier from Election Systems and Software several years ago. ES&S still sells and services Premier equipment along with its own system, but Dominion owns the intellectual property rights of Premier equipment as a result of its purchase of the company.

As of this writing, Secretary Kobach has not certified the Dominion Democracy Suite. CEOs will be notified if and when certification is granted.

The Democracy Suite is a paper optical scan-based system which includes precinct ballot scanners and central scanners. The accessible ADA- and HAVA-compliant device allows a voter with a visual impairment to record his/her choices using an audio ballot and keypad. The system prints an optical scan ballot that is scanned along with other ballots. ■

Sedgwick County Sued Over Ballot Records

Sedgwick County Election Commissioner Tabitha Lehman was sued by a person seeking public access to Real Time Audit Logs (RTALs) on electronic voting machines. RTAL is ES&S's trade name for a voter verifiable paper audit trail (VVPAT), which is a printable electronic record of each voter's actions on the voting machine. RTAL documents are viewable by the voter before the electronic ballot is cast. Once the voter has cast the ballot the documents are randomly stored in the system's memory.

Elizabeth Clarkson v. Sedgwick County Elections Commissioner Tabitha Lehman was filed in state district court in Sedgwick County on June 18, 2013. The plaintiff sought access to RTAL records pursuant to the Kansas Open Records Act in order to conduct a post-election audit of the results of the November 2010 election.

In response to the plaintiff's original request for records, the election office provided precinct-based results tapes but denied the request for individual ballot logs, citing K.S.A. 25-2422 and the unnecessary burden and expense required to produce the records. State law does provide limited access to election records in a recount, but the law does not have specific provisions related to VVPATs or RTALs. These arguments were detailed in a response filed in court in July.

The court ruled in favor of the election commissioner's office. ■

SOS Holiday Hours

In observance of the regular calendar of state holidays, the secretary of state's office will be closed on the following dates:

December 25, 2013, for Christmas Day, and **January 1, 2014,** for New Year's Day.

In addition, the office will be closed Monday, **January 20, 2014** in observance of Martin Luther King, Jr. Day.

Happy Holidays from the SOS office!

Exhibit 34

Interstate Voter Registration Crosscheck Program

National Association of State Election Directors

January 26, 2013

Kris W. Kobach

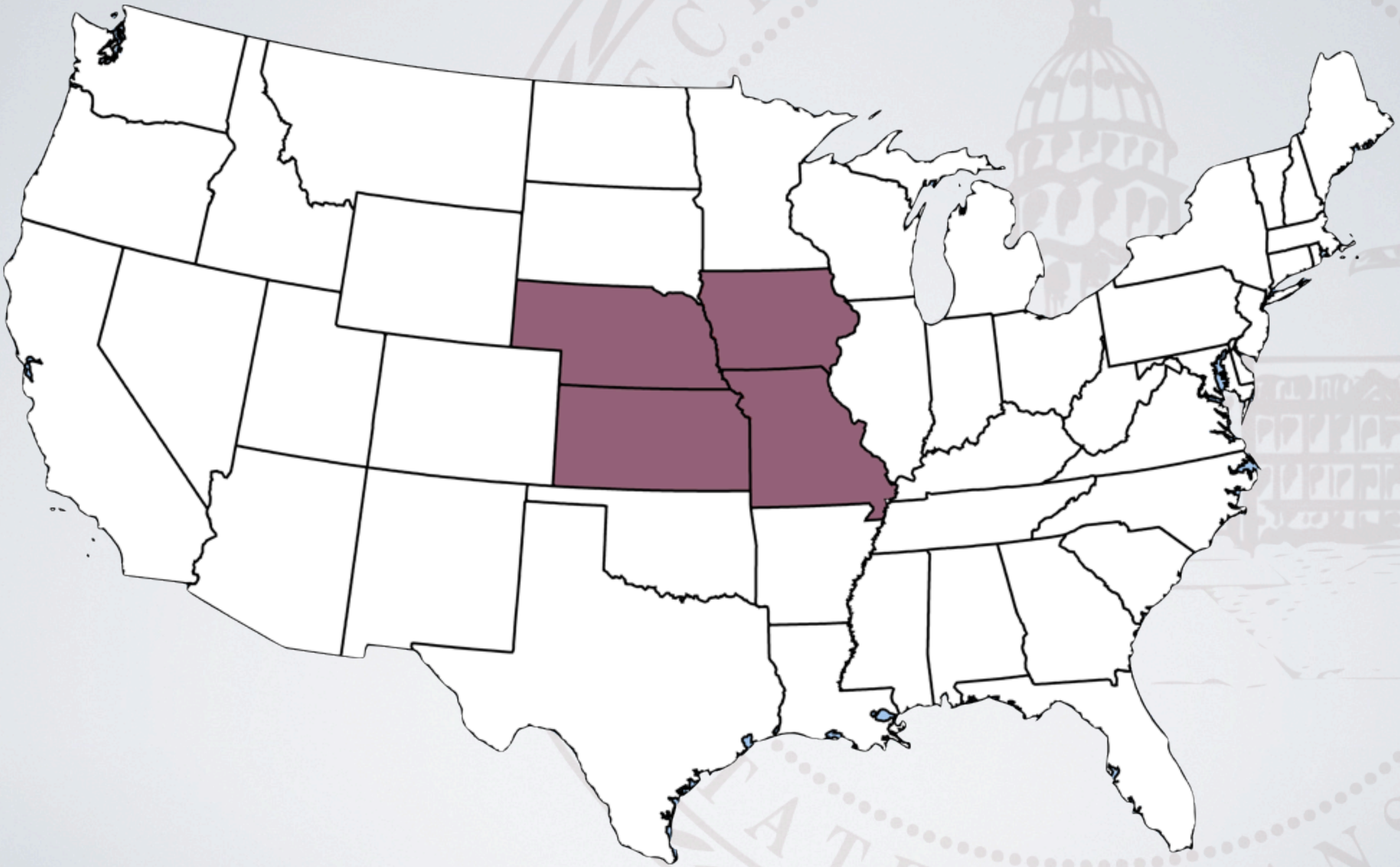
National Voter Registration Act of 1993

- **Section 2 Findings and Purposes**
- (b) Purposes
- (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office;
- (2) to make it possible for Federal, State, and local governments to implement this subchapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
- (3) to protect the integrity of the electoral process; and
- **(4) to ensure that accurate and current voter registration rolls are maintained.**

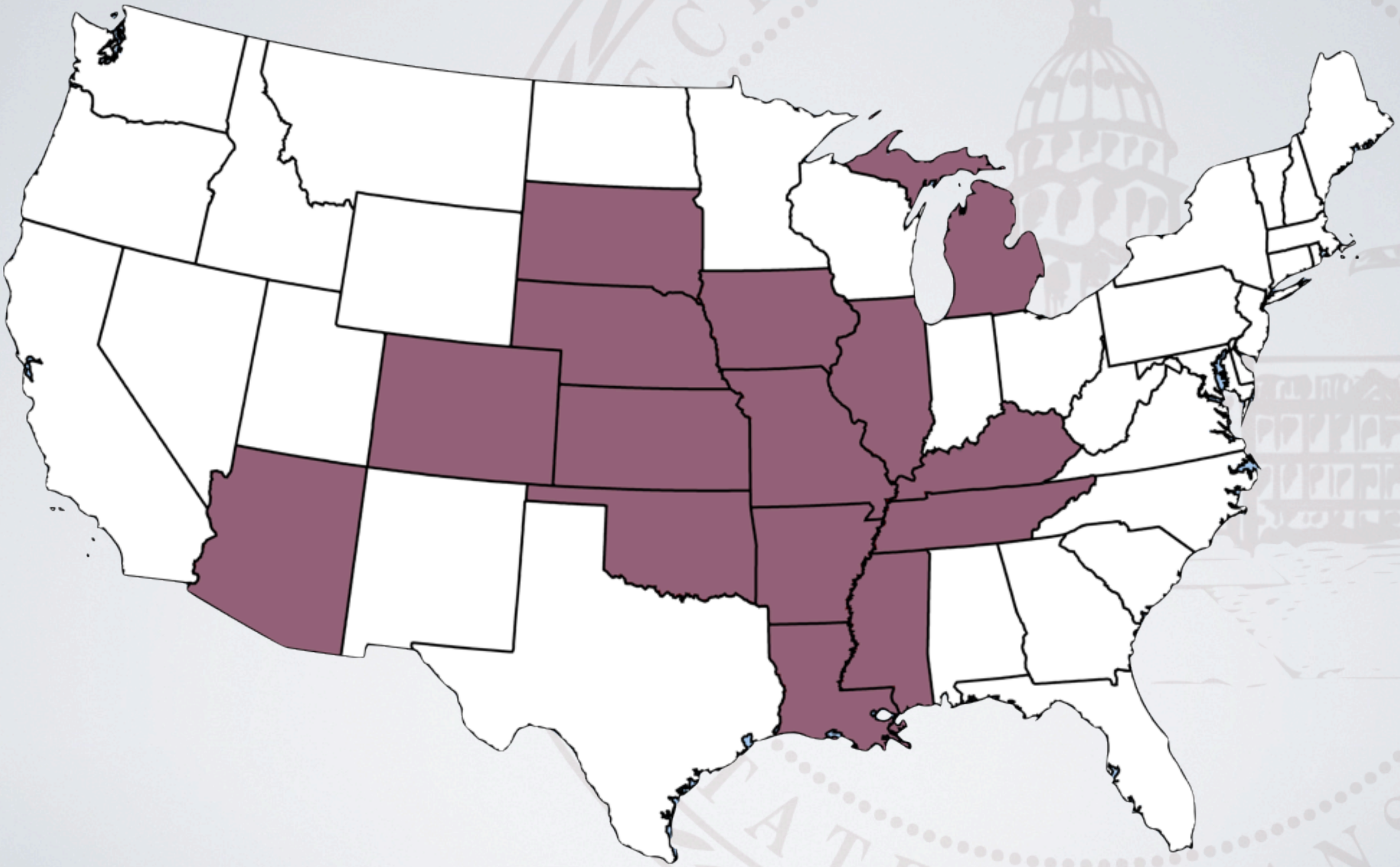
From the Federal Election Commission's guide: Implementing the National Voter Registration Act of 1993:

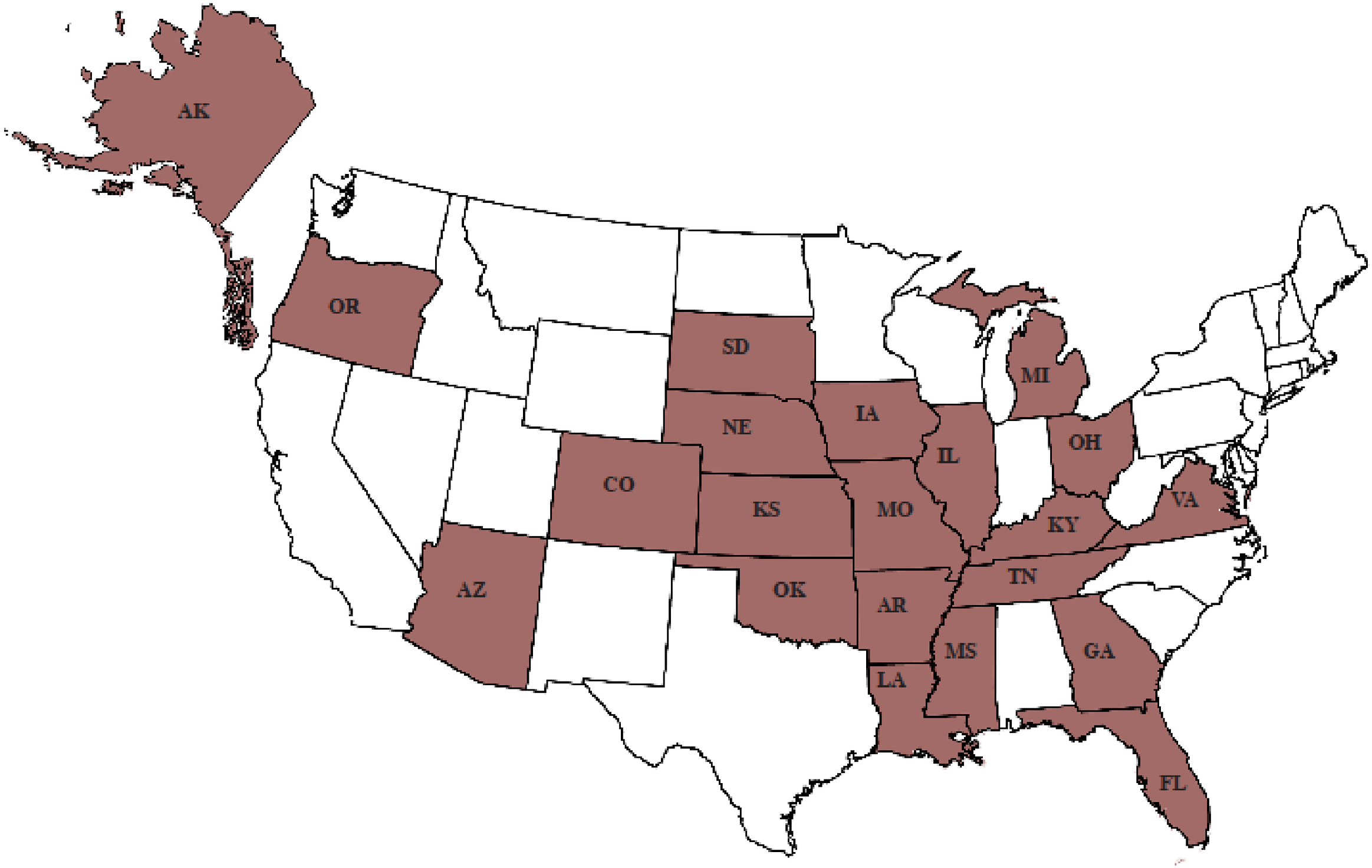
The features (of the National Voter Registration Act) include a requirement that states "conduct a general program" the purpose of which is "to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office"

Participants in 2005



Participants in 2012





2013 Interstate Crosscheck

Participating states as of Jan. 10, 2013

2012 Crosscheck Program—Number of Records Compared

Arizona	3,545,891	Michigan	7,337,846
Arkansas	1,528,458	Mississippi	2,002,406
Colorado	3,375,891	Missouri	4,069,576
Illinois	8,248,736	Nebraska	1,129,943
Iowa	2,113,199	Oklahoma	2,000,767
Kansas	1,702,495	South Dakota	560,147
Kentucky	1,303,684	Tennessee	3,468,503
Louisiana	2,860,281		

Total Records: 45,247,823

Interstate Crosscheck Data Format

Field	Format	Example
Status	A=Active; I=Inactive	A
Date_Generated	YYYY/MM/DD	2010/01/01
First_Name		Bob
Middle_Name		Alan
Last_Name		Jones
Suffix Name		Jr
Date_of_Birth	YYYY/MM/DD	1940/06/16
Voter_ID_Number		123456
Last_4_SSN		7890
Mailing Address	Line 1 Line 2 City State Zip	123 Anywhere St...
County		Allen
Date_of_Registration	YYYY/MM/DD	1970/01/01
Voted_in_2010	Y=did vote; N=did not vote	Y

How does it work?

- Each state pulls data on January 15 each year using prescribed data format
- Upload data to secure FTP site (hosted by Arkansas)
- Kansas IT department pulls data, runs comparison, uploads results to FTP site
- Each state downloads results from FTP site, processes them according to state laws & regulations
- Kansas deletes all other states' data

First: John
Middle: Q.
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Kansas

First: John
Middle:
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Colorado

Potential match

Grid of Potential Duplicate Voters Within States
by DOB Last Name First Name

2012	AZ	AR	CO	IL	IA	KS	KY	LA	MI	MS	MO	NE	OK	SD	TN
AZ		2,829	24,863	16,014	7,153	3,687	688	2,062	27,617	2,220	7,569	3,306	4,006	2,449	3,614
AR	2,829		4,557	6,950	2,430	2,686	691	5,957	5,085	6,477	11,049	995	7,403	433	7,180
CO	24,863	4,557		19,902	10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IL	16,014	6,950	19,902		31,882	6,311	2,467	5,207	49,260	10,766	39,658	3,803	4,834	1,500	12,469
IA	7,153	2,430	10,850	31,882		4,706	526	1,558	7,019	1,797	11,563	10,954	2,031	4,865	2,806
KS	3,687	2,686	10,035	6,311	4,706		401	1,369	4,461	1,397	31,082	4,196	6,575	905	2,205
KY	688	691	1,054	2,467	526	401		873	2,267	1,085	1,195	233	576	117	1,905
LA	2,062	5,957	5,065	5,207	1,558	1,369	873		6,851	17,744	5,254	810	2,829	277	4,422
MI	27,617	5,085	17,086	49,260	7,019	4,461	2,267	6,851		7,527	12,960	2,416	4,067	1,265	16,956
MS	2,220	6,477	3,309	10,766	1,797	1,397	1,085	17,744	7,527		5,607	780	2,364	305	21,661
MO	7,569	11,049	12,498	39,658	11,563	31,082	1,195	5,254	12,960	5,607		4,244	7,539	1,300	7,804
NE	3,306	995	8,927	3,803	10,954	4,196	233	810	2,416	780	4,244		1,126	2,608	1,108
OK	4,006	7,403	8,306	4,834	2,031	6,575	576	2,829	4,067	2,364	7,539	1,126		402	2,858
SD	2,449	433	3,937	1,500	4,865	905	117	277	1,265	305	1,300	2,608	402		537
TN	3,614	7,180	6,153	12,469	2,806	2,205	1,905	4,422	16,956	21,661	7,804	1,108	2,858	537	
Totals	**108,077**	**64,722**	**136,542**	**211,023**	**100,140**	**80,016**	**14,078**	**60,278**	**164,837**	**83,039**	**159,322**	**45,506**	**54,916**	**20,900**	**91,678**

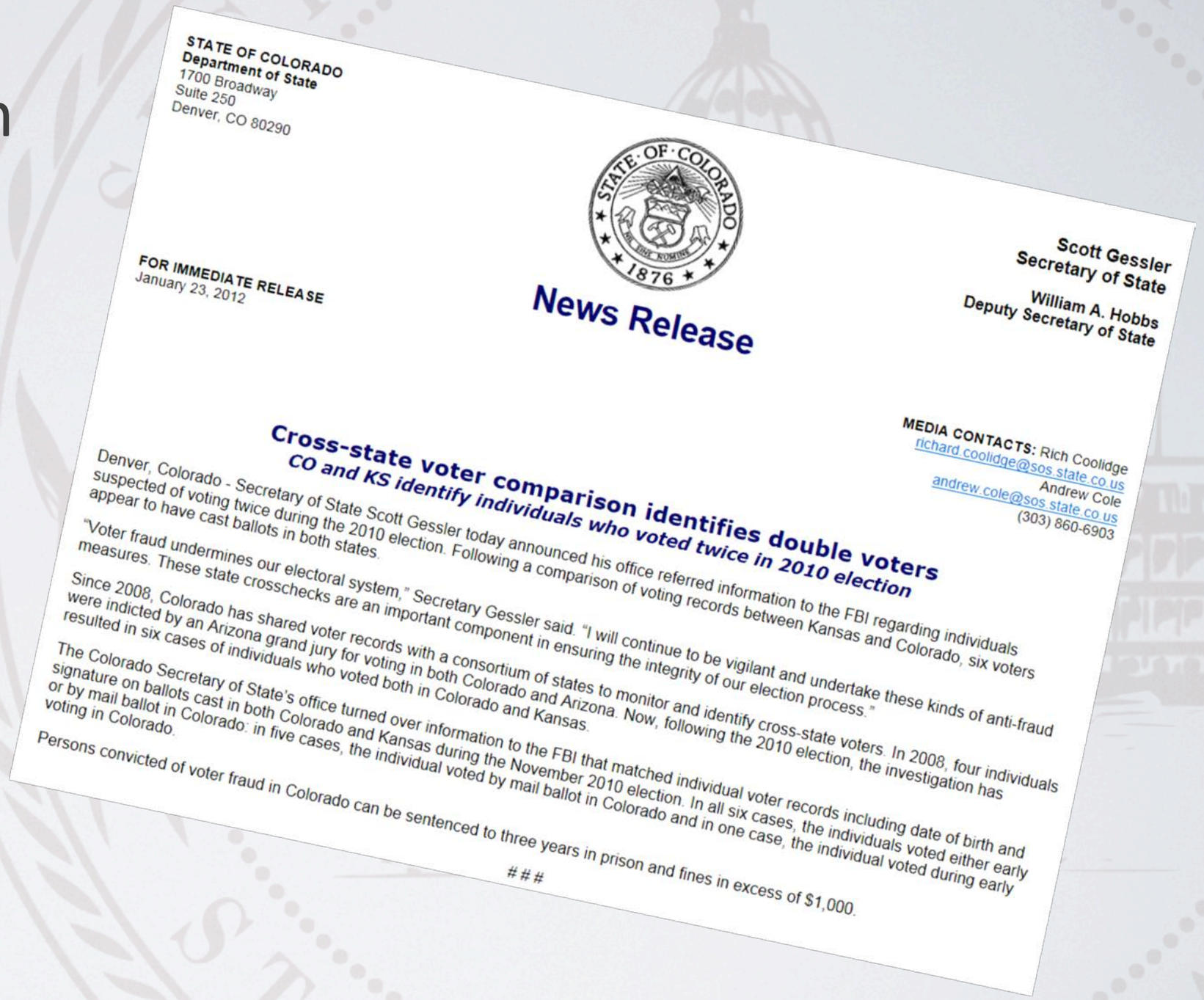
Success in Kansas

Double Votes from 2008 and 2010 Referred to Prosecution Discovered through Interstate Crosscheck Program	
2008	**2010**
Kansas - Kentucky	Kansas – Arkansas (2)
Kansas - Colorado	Kansas – Colorado (5)
Kansas - Kansas	Kansas – Iowa
	Kansas – Louisiana
	Kansas – Nebraska
	Kansas - Oklahoma

Success in other states - Colorado

- Four individuals indicted for voting in Colorado and Arizona in first year of participation

- Six additional cases of double voting referred to FBI in 2012



STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Scott Gessler
Secretary of State

William A. Hobbs
Deputy Secretary of State

FOR IMMEDIATE RELEASE
January 23, 2012

News Release

MEDIA CONTACTS: Rich Coolidge
richard.coolidge@sos.state.co.us
Andrew Cole
andrew.cole@sos.state.co.us
(303) 860-6903

Cross-state voter comparison identifies double voters
CO and KS identify individuals who voted twice in 2010 election

Denver, Colorado - Secretary of State Scott Gessler today announced his office referred information to the FBI regarding individuals suspected of voting twice during the 2010 election. Following a comparison of voting records between Kansas and Colorado, six voters appear to have cast ballots in both states.

"Voter fraud undermines our electoral system," Secretary Gessler said. "I will continue to be vigilant and undertake these kinds of anti-fraud measures. These state crosschecks are an important component in ensuring the integrity of our election process."

Since 2008, Colorado has shared voter records with a consortium of states to monitor and identify cross-state voters. In 2008, four individuals were indicted by an Arizona grand jury for voting in both Colorado and Arizona. Now, following the 2010 election, the investigation has resulted in six cases of individuals who voted both in Colorado and Kansas.

The Colorado Secretary of State's office turned over information to the FBI that matched individual voter records including date of birth and signature on ballots cast in both Colorado and Kansas during the November 2010 election. In all six cases, the individuals voted either early or by mail ballot in Colorado: in five cases, the individual voted by mail ballot in Colorado and in one case, the individual voted during early voting in Colorado.

Persons convicted of voter fraud in Colorado can be sentenced to three years in prison and fines in excess of $1,000.

###

Kris W. Kobach

What does it cost to participate?

$0

Kris W. Kobach

How Can a State Join the Crosscheck?

1. Chief State Election Official signs the Memorandum of Understanding (MOU)

2. CSEO assigns two staff members:
   - one election administration person
   - one IT person

3. Staff members will:
   - participate in annual conference call and email
   - pull VR data in January
   - receive cross check results and process
   - instruct local elections officials (respond to requests for addresses, signatures on poll books, etc.)

Contact

Brad Bryant
State Election Director
Kansas Secretary of State's Office
brad.bryant@sos.ks.gov
785-296-4561

Kris W. Kobach

Exhibit 35

The GOP's Stealth War Against Voters

Will an anti-voter-fraud program designed by one of Trump's advisers deny tens of thousands their right to vote in November?

The Crosscheck program is a response to the imaginary menace of mass voter fraud. Mark Makela/Reuters

By Greg Palast
August 24, 2016

When Donald Trump claimed, "the election's going to be rigged," he wasn't entirely wrong. But the threat was not, as Trump warned, from Americans committing the crime of "voting many, many times." What's far more likely to undermine democracy in November is the culmination of a decade-long Republican effort to disenfranchise voters under the guise of battling voter fraud. The latest tool: Election officials in more than two dozen states have compiled lists of citizens whom they allege could be registered in more than one state – thus potentially able to cast multiple ballots – and eligible to be purged from the voter rolls.

The data is processed through a system called the Interstate Voter Registration Crosscheck Program, which is being promoted by a powerful Republican operative, and its lists of potential duplicate voters are kept confidential. But *Rolling Stone* obtained a portion of the list and the names of 1 million targeted voters. According to our analysis, the Crosscheck list disproportionately threatens solid Democratic constituencies: young, black, Hispanic and Asian-American voters – with some of the biggest possible purges underway in Ohio and North Carolina, two crucial swing states with tight Senate races.

RELATED

2016: First Presidential Election Since Voting Rights Gutted
America will vote for president in a country where it's easier to buy a gun than vote in many states

Like all weapons of vote suppression, Crosscheck is a response to the imaginary menace of mass voter fraud. In the mid-2000s, after the Florida-recount debacle, the Bush administration launched a five-year investigation into the allegedly rampant crime but found scant evidence of wrongdoing. Still, the GOP has perpetuated the myth in every national election since. Recently, North Carolina Board of Elections chief Kim Strach testified to her legislature that 35,750 voters are "registered in North Carolina and another state and voted in both in the 2012 general election." [Editor's note: This quote was taken from the power point that accompanied Strach's testimony. In a subsequent letter, she informed us that during her presentation she "stressed that we were not suggesting that 35,750 voters had committed any type of fraud. My testimony was that the data we received from the Crosscheck Program showed that in the 2012 general election, there were 35,750 people who voted in North Carolina whose first and last names and dates of birth matched persons who voted in the same election in another state."] Yet despite hiring an ex-FBI agent to lead the hunt, the state has charged exactly zero double voters from the Crosscheck list. Nevertheless, tens of thousands face the loss of their ability to vote – all for the sake of preventing a crime that rarely happens. So far, Crosscheck has tagged an astonishing 7.2 million suspects, yet we found no more than four perpetrators who have been charged with double voting or deliberate double registration.

On its surface, Crosscheck seems quite reasonable. Twenty-eight participating states share their voter lists and, in the name of dispassionate, race-blind Big Data, seek to ensure the rolls are up to date. To make sure the system finds suspect voters, Crosscheck

supposedly matches first, middle and last name, plus birth date, and provides the last four digits of a Social Security number for additional verification.

In reality, however, there have been signs that the program doesn't operate as advertised. Some states have dropped out of Crosscheck, citing problems with its methodology, as Oregon's secretary of state recently explained: "We left [Crosscheck] because the data we received was unreliable."

In our effort to report on the program, we contacted every state for their Crosscheck list. But because voting twice is a felony, state after state told us their lists of suspects were part of a criminal investigation and, as such, confidential. Then we got a break. A clerk in Virginia sent us its Crosscheck list of suspects, which a letter from the state later said was done "in error."

The Virginia list was a revelation. In all, 342,556 names were listed as apparently registered to vote in both Virginia and another state as of January 2014. Thirteen percent of the people on the Crosscheck list, already flagged as inactive voters, were almost immediately removed, meaning a stunning 41,637 names were "canceled" from voter rolls, most of them just before Election Day.

We were able to obtain more lists – Georgia and Washington state, the total number of voters adding up to more than 1 million matches – and Crosscheck's results seemed at best deeply flawed. We found that one-fourth of the names on the list actually lacked a middle-name match. The system can also mistakenly identify fathers and sons as the same voter, ignoring designations of Jr. and Sr. A whole lot of people named "James Brown" are suspected of voting or registering twice, 357 of them in Georgia alone. But according to Crosscheck, James Willie Brown is supposed to be the

same voter as James Arthur Brown. James Clifford Brown is allegedly the same voter as James Lynn Brown.

And those promised birth dates and Social Security numbers? The Crosscheck instruction manual says that "Social Security numbers are included for verification; the numbers might or might not match" – which leaves a crucial step in the identification process up to the states. Social Security numbers weren't even included in the state lists we obtained.

We had Mark Swedlund, a database expert whose clients include eBay and American Express, look at the data from Georgia and Virginia, and he was shocked by Crosscheck's "childish methodology." He added, "God forbid your name is Garcia, of which there are 858,000 in the U.S., and your first name is Joseph or Jose. You're probably suspected of voting in 27 states."

Swedlund's statistical analysis found that African-American, Latino and Asian names predominate, a simple result of the Crosscheck matching process, which spews out little more than a bunch of common names. No surprise: The U.S. Census data shows that minorities are overrepresented in 85 of 100 of the most common last names. If your name is Washington, there's an 89 percent chance you're African-American. If your last name is Hernandez, there's a 94 percent chance you're Hispanic. If your name is Kim, there's a 95 percent chance you're Asian.

The Crosscheck program, started by Kris Kobach, has spread to over two dozen states, tagging more than 7 million voters as possibly suspect. Christopher Smith/Washington Post/Getty

This inherent bias results in an astonishing one in six Hispanics, one in seven Asian-Americans and one in nine African-Americans in Crosscheck states landing on the list. Was the program designed to target voters of color? "I'm a data guy," Swedlund says. "I can't tell you what the intent was. I can only tell you what the

outcome is. And the outcome is discriminatory against minorities."

Every voter that the state marks as a legitimate match receives a postcard that is colorless and covered with minuscule text. The voter must verify his or her address and mail it back to their secretary of state. Fail to return the postcard and the process of taking your name off the voter rolls begins.

This postcard game amplifies Crosscheck's built-in racial bias. According to the Census Bureau, white voters are 21 percent more likely than blacks or Hispanics to respond to their official requests; homeowners are 32 percent more likely to respond than renters; and the young are 74 percent less likely than the old to respond. Those on the move – students and the poor, who often shift apartments while hunting for work – will likely not get the mail in the first place.

At this point, there's no way to know how each state plans to move forward. If Virginia's 13 percent is any indication, almost 1 million Americans will have their right to vote challenged. Our analysis suggests that winding up on the Crosscheck list is hardly proof that an individual is registered in more than one state. Based on the data, the program – whether by design or misapplication – could save the GOP from impending electoral annihilation. And not surprisingly, almost all Crosscheck states are Republican-controlled.

The man behind crosscheck is Kansas Secretary of State Kris Kobach, a Yale-educated former law professor. After 9/11, U.S. Attorney General John Ashcroft tasked Kobach with creating a system to track foreign travelers. (It was later shut down over concerns about racial profiling.) He is best known as the author of Arizona's "Driving While Brown Law," which allowed cops to pull over drivers and ask for proof of their legal status. He co-wrote the ultraconservative 2016 RNC

party platform, working in a recommendation that Crosscheck be adopted by every state in the Union. He's also the Trump adviser who came up with a proposal to force Mexico into paying for Trump's wall.

In January 2013, Kobach addressed a gathering of the National Association of State Election Directors about combating an epidemic of ballot-stuffing across the country. He announced that Crosscheck had already uncovered 697,537 "potential duplicate voters" in 15 states, and that the state of Kansas was prepared to cover the cost of compiling a nationwide list. That was enough to persuade 13 more states to hand over their voter files to Kobach's office.

In battleground-state Ohio, Republican Secretary of State John Husted's Crosscheck has flagged close to half a million voters. In Dayton, we tracked down several of the suspects on our lists. Hot spots of "potential duplicate" voters, we couldn't help but notice, were in neighborhoods where the streets are pocked with rundown houses and boarded storefronts. On Otterbein Avenue, I met Donald Webster, who, like most in his neighborhood, is African-American.

Crosscheck lists him registered in Ohio as Donald Alexander Webster Jr., while registered a second time as Donald *Eugene*Webster (no "Jr.") in Charlottesville, Virginia. Webster says he's never been a "Eugene" and has never been to Charlottesville. I explained that both he and his Virginia doppelgänger were subject to losing their ability to vote.

"How low can they go?" he asked. "I mean, how can they do that?"

I put his question to Robert Fitrakis, a voting-rights attorney who examined our Crosscheck data. I showed him Donald Webster's listing – and page after page of Ohio voters. Fitrakis says that the Ohio secretary of state's enthusiasm for Crosscheck fits a pattern: "He

doesn't want to match middle names, because he doesn't want real matches. They're targeting people with clearly defined ethnic names that typically vote for the Democratic Party. He wants to win Ohio the only way he knows how – by taking away the rights of citizens to vote."

Kobach refused to speak for this story. So I went to Newton, Kansas, where he was headlining an ice-cream-social fundraiser in a public park. I approached Kobach with the Crosscheck list he had refused me, and asked, "Why are these lists so secret?"

RELATED
Watch John Oliver's Takedown of Voter ID Laws
"It's just one of those things that white people are more likely to have. Like a sunburn. Or an Oscar nomination," host says of IDs

"They aren't," Kobach answered, contradicting what his attorney had told me.

I pointed to a random match on the Crosscheck list and asked him why it identified James *Evans* Johnson as the same voter as James P. Johnson.

Kobach denied the name could be on the list. "Our system would not yield this match," he said. (And according to the rules of his program, it shouldn't have.)

"This is the list you gave [Virginia], and they knocked off 41,000 voters," I said.

"That is false!" he said, as he hurried away. "You know why? Federal law prohibits that."

Kobach is correct that federal regulation typically would complicate such a sweeping purge, but somehow tens of thousands of voters in Virginia got knocked off the rolls anyway.

Kobach's Crosscheck purge machinery was in operation well before Trump arrived on the political scene – and will continue for elections to come. Low voter turnout of any kind traditionally favors the GOP, and this is the party's long game to keep the rolls free of young people, minorities and the poor. Santiago Juarez of New Mexico, an attorney who has done work for the League of United Latin American Citizens, has spent years signing up Hispanic voters in the face of systemic efforts to suppress their vote. He scoffed at the idea of a massive conspiracy among Latinos to vote in two states. "Hell," he said, "you can't get people to vote once, let alone twice."

Exhibit 36

Report to Congress – December 2016

Table of Contents

Section 1

Introduction

In August 2014, the United States Digital Service (USDS) was created to improve the Federal Government's most important public-facing digital services. USDS is a collaboration between some of the country's top technical talent and the government's brightest civil servants, who work in partnership to apply private sector best practices to our digital services.

Initially, USDS' small team of technologists planned to focus on three projects. Additional funding and the support of Congress for the Information and Technology Oversight and Reform (ITOR) Fund in the 2015 and 2016 Fiscal Year appropriations bills allowed USDS to invest in a greater number of high-priority projects, detailed in this report. Of the $30M appropriated in the 2016 fiscal year, $14M was apportioned to USDS to support its operations, with the balance of the $30M supporting other IT oversight and reform activities. At its creation, USDS was administratively placed within the Office of the Federal CIO. After more than two years of operations, however, the Office of Management and Budget (OMB) has decided to move the Administrator of USDS to directly report to the Deputy Director of Management (DDM).

USDS staff in OMB work alongside agency Digital Service team staff to support high-priority projects in agencies including the Departments of Veterans Affairs, State, Education, Homeland Security, Health and Human Services, Defense, the Internal Revenue Service, and the Small Business Administration.

The central focus of USDS is on the measurable improvement of the performance and cost-effectiveness of important, public-facing Federal Government digital services – via the application of modern technology best practices. To execute this mission, USDS conducts hands-on engagements with agencies. A summary of USDS' most impactful engagements is provided in Section 2.

In support of its core mission of improving the performance and cost-effectiveness of important government digital services, the USDS engages in three additional activities:

- **Rethink how we build and buy digital services.** USDS is working on modernizing procurement processes and practices for the modern digital era. Our partners in the IT contracting community are a critical element of modernizing our government, as skilled contractors deliver the majority of the government's digital services.
- **Expand the use of common platforms, services and tools.** USDS is working with agencies to identify and implement shared tools and services to address common technical issues and usability challenges across the Federal Government. One example is building Login.gov, a universal login system that will enable the

American public to access multiple government agency services with one, streamlined account.

- **Bring top technical talent into public service.** In support of these goals, USDS has recruited and placed over 200 Digital Service Experts, from one of the most competitive industries in the world, to join the government for term-limited tours of duty with the USDS and work with civil servants inside agencies. The long-term goal is to encourage a tradition of public service in the tech industry that will support the ongoing improvement of government digital services.

USDS has developed procedures and criteria for prioritizing projects, which includes obtaining input from OMB's IT Dashboard, agency leadership, and relevant U.S. Government Accountability Office (GAO) reports. To prioritize projects, USDS also uses the following three criteria, which are listed in their order of importance:

(1) What will do the greatest good for the greatest number of people in the greatest need?
(2) How effective and cost-efficient will the USDS investment be?
(3) What potential exists to use or reuse a technological solution across the Federal Government?

Along with its investment in the ITOR Fund, Congress asked USDS to provide a regular update on progress in each of its programs. This report details that progress.

Mikey Dickerson
Administrator, U.S. Digital Service

Section 2

High Priority Projects

Priority Project Summary

USDS executes focused, hands-on engagements in which small teams of technical experts embed into existing agency programs, where they accelerate adoption of modern private sector best practices on important projects. These engagements may be proactive or reactive, and can range from two-week diagnostic sprints to in-depth multi-month engagements to dramatically improve a target service.

Typically, USDS is focused on increasing the success rate of a major IT acquisition in an agency. USDS personnel help promote the critical factors underlying successful major IT acquisitions identified by GAO in 2011 and reiterated in 2015 by GAO in its report on "Improving the Management of IT Acquisitions and Operations."

This section details USDS' most impactful projects, including those completed during the 2016 Fiscal Year:

- **Stabilizing and Improving HealthCare.gov (page 9).** In the 2013-2014 Open Enrollment season, a small team of private sector experts helped overhaul, update, and simplify the design and infrastructure of HealthCare.gov, helping eight million Americans sign up for coverage. This success paved the way for the creation of USDS. In the two subsequent open enrollment periods, USDS staff continued to partner with CMS staff and contractors to further improve the HealthCare.gov system and services.
- **Modernizing the Immigration System at DHS (page 14).** Since 2014, USDS has been helping USCIS implement private sector best practices on the Electronic Immigration System project. As of September 2016, 25% of immigration transactions applications are processed electronically using the system, including the green card renewal application (I-90), which has a 92% user satisfaction rate.
- **Streamlining VA Disability Claim Processing (page 20).** Over the summer of 2016, the USDS team at VA helped launch Caseflow Certification, a tool to improve paperless appeals processing by detecting if required documentation has been added before an appeal can move forward. This simple check helps reduce preventable errors and avoidable delays caused by disjointed, manual processing. As of September 2016, approximately 87% of all paperless appeals are certified using the tool.
- **Simplifying Veteran-facing Services with Vets.gov (page 26).** USDS is working with leaders across VA to build Vets.gov, a simple, easy-to-use site that consolidates information for Veterans. Over the summer, the USDS team helped VA launch a new digital application for healthcare built with feedback from

Veterans. Previously, less than 10 percent of applicants applied online. Since the launch of the new healthcare application, daily online applications have increased from 62 per day to more than 500 per day.

- **Providing Secure Access to IRS Taxpayer Information (page 31).** USDS helped IRS introduce Secure Access in June 2016, a user verification process that relies on strong identity proofing and two-factor authentication to protect users' sensitive tax records. Secure Access ensures that users have convenient, real-time access to their transcripts while protecting taxpayer information from automated fraudulent attacks. As of September 2016, taxpayers have accessed 2.7 million tax records using the Secure Access process.
- **Improving the Visa Processing System at Department of State (page 37).** USDS is assisting State to implement improvements in the Consolidated Consular Database, on which many Visa processing applications depend. USDS helped State adopt modern engineering best practices, and is helping State develop tools to communicate case status to applicants, which is the primary reason for many of the 9,000 phone calls the National Visa Center receives per day.
- **Helping CMS Implement Congressionally Mandated Medicare Payment Changes (page 41).** Implementation of the Medicare Access and Chip Reauthorization Act of 2015 (MACRA) will change the way Medicare pays doctors for services rendered to Medicare patients. USDS is helping CMS use modern best practices to ensure the transition from the current payment program to the new system is simple, clear and effective.
- **Reducing Inefficiency in the Refugee Admission Process (page 44).** Each year, the United States admits tens of thousands of refugees using a rigorous approval process. Previously, DHS officers had to approve refugee registration forms using an ink approval stamp in the field where the refugee file was physically located. USDS helped DHS and State implement a "digital stamp," removing an unnecessary processing delay of 2 to 8 weeks for thousands of cases.
- **Helping Students Make More Informed College Choices at Department of Education (page 49).** USDS, along with 18F, helped the Department of Education launch the College Scorecard to help students make more informed decisions about college selection. Millions of students have already benefited from this data, the most comprehensive and reliable ever published on employment outcomes and success in repaying student loans. Additionally, more than a dozen organizations have built new tools using the data.
- **Modernizing the Department of Defense Travel System (page 55).** The USDS team at DoD (Defense Digital Service) is helping implement a new commercial

tool to better manage the $3.5 billion of travel handled through the Defense Travel System each year.

- **Identifying Security Vulnerabilities in Department of Defense Websites (page 59).** To strengthen data security at DoD, the USDS team at DoD (Defense Digital Service) launched "Hack the Pentagon," the first bug bounty program in the history of the Federal Government. Adopting this private sector best practice led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000, compared to the $1 million DoD estimates contracting an outside firm to do a similar audit would have cost.

Additional detail on each of these projects is provided in the chapters below.

Stabilizing and Improving HealthCare.gov

The Challenge

As required by the Affordable Care Act, HealthCare.gov is the Federal website that facilitates purchase of private health insurance for consumers who reside in states that did not establish health insurance marketplaces. HealthCare.gov supports the Federal Health Insurance Marketplace (Marketplace), providing citizens with the ability to compare, shop for, and enroll in affordable healthcare plans.

HealthCare.gov launched in October 2013, and encountered serious technical challenges which prevented many people from using the service.

Project Impact Summary

- A team of private sector engineers and product managers joined CMS staff and contractors to identify and solve website operation problems. By March 2014, over 8 million Americans had successfully signed up for health insurance and the site was stable.
- In the two subsequent open enrollment periods, USDS staff continued to partner with CMS to improve the HealthCare.gov system and services. USDS staff helped CMS implement several private sector best practices including performance tracking of the system and application process, building an improved identity management solution with an uptime of 99.99%, increasing the conversion rate in the new application workflow from 55% to 85%, and building new systems with industry standard open source software.

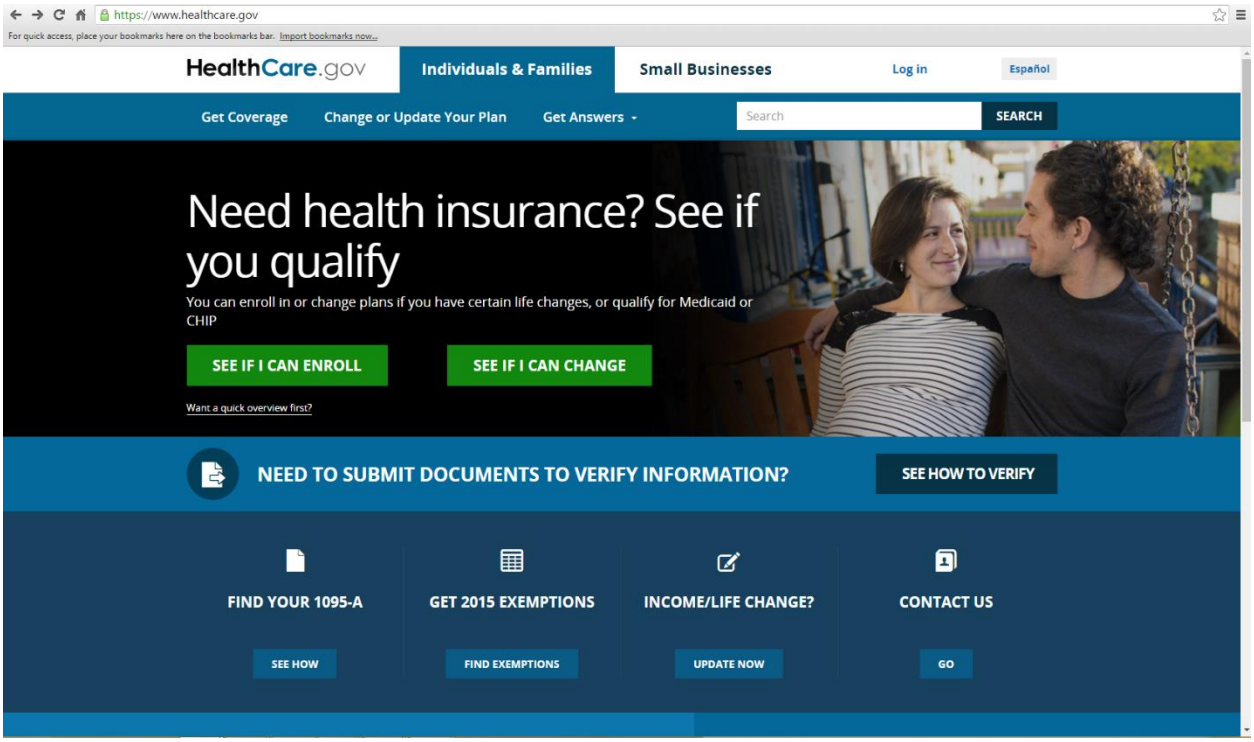
The Solution

Over the three month period following the launch, a team of engineers and product managers from the private sector joined with CMS staff and existing contractor teams to troubleshoot the service. Working around the clock, this “tech surge” team systematically identified and solved problems with the service by following industry best practices in site reliability and product management. By March 2014, the end of the Marketplace’s first open enrollment period, over 8 million Americans had successfully signed up for health insurance.

The HealthCare.gov turn-around demonstrated the enormous potential of empowering small teams of America’s brightest digital talent to apply modern technology best

practices to Federal Government projects. In August 2014, the White House established the U.S. Digital Service (USDS) to apply this technique to a greater number of projects. Mikey Dickerson, a site reliability engineer on the HealthCare.gov team, was appointed the USDS Administrator.

In the two subsequent open enrollment periods (ending February 2015 and January 2016), USDS engineers, product managers and designers partnered with CMS staff to continue to improve HealthCare.gov systems and processes used to deliver the service.



For example, contractors from multiple companies along with CMS staff improved coordination in the Healtchare.gov operations center by embracing a “one-team” mentality with fewer process restrictions, which has improved the ability of this team to troubleshoot issues and make important decisions quickly. The team also implemented application monitoring to track performance.

Additionally, USDS supported several smaller teams working on components of HealthCare.gov which adopted agile and iterative development processes, allowing them to quickly deliver functioning software. In one such case, a small team built and launched the Scalable Login System (SLS), a replacement for HealthCare.gov’s previous identity management solution. SLS has proven to be vastly more stable and efficient since it was created specifically for use by Marketplace consumers.

Additionally, CMS launched a simpler and more efficient application for healthcare plan enrollment (Marketplace Lite 2.0 App). The conversion rate in the new application workflow stands at around 85%, compared with approximately 55% in the previous system. Finally, CMS with input from the insurer community, built and launched a new set of decision support tools for the window shopping and plan compare tools. These tools allow consumers to search for preferred doctors, prescription drugs, and facilities while shopping for a health plan. This was one of the most requested features from Marketplace consumers over the past several years.

Success Criteria	Status
Transition HealthCare.gov to a scalable login system with an uptime of 99% or greater	Complete. Scalable Login System implemented and users migrated to the system in 2015. Uptime 99.99%
Implement application monitoring.	Complete. Monitoring installed and in use.
Launch the Marketplace Lite 2.0 app	Complete. App launched in 2015, resulting in improved conversion rates.

Milestones

- October 2013: HealthCare.gov launches. “Tech surge” assists with troubleshooting the service.
- March 2014: First open enrollment period closes with 8 million Americans enrolled (5.3 million through HealthCare.gov).
- August 2014: USDS created.
- November 2014: Second open enrollment period begins. USDS team supports Marketplace operations.
- February 2015: Second open enrollment period ends with 11.7 million enrollments (8.8 million through HealthCare.gov). USDS team supports Marketplace operations and assists with the transition from to SLS.
- November 2015: Third open enrollment period begins. USDS team supports Marketplace operations
- January 2016: Third open enrollment period ends with 12.7 million enrollments (9.6 million through HealthCare.gov). USDS support role winds down.

The Process and Lessons Learned

1. **Install application monitoring.** At initial launch of HealthCare.gov, there was no end-to-end monitoring of the production system, making identification, prioritization and diagnosis of errors very challenging. One of the first actions the "tech surge" team took was to recommend the addition of an application monitoring tool, which has remained an important resource for the team to identify issues as they occur.

2. **Facilitate open and direct communication between technical contributors.** HealthCare.gov has many components, many of which were created by different companies hired by CMS. Problems with the integration of these components was a source of many errors in the initial launch. The most effective solution was to bring individual technical contributors from these various teams to a single location where problems could be discussed openly, solutions could be explored, and assignments could be made. Additionally, all staff and contractors working on aspects of HealthCare.gov began to use a collaboration tool to communicate more effectively.

3. **Deploy in a flexible hosting environment.** Traffic on HealthCare.gov is highly variable. Near the end of an enrollment period, for example, the number of visitors can increase by an order of magnitude.

   Several of the newer components of HealthCare.gov are deployed in a flexible cloud hosting environment (including SLS and the Marketplace Lite App 2.0 described above). CMS has experienced high availability and increased development speeds with this approach, and is seeking to use this approach for more of its components.

4. **Build services using agile and iterative processes.** CMS has had success using small teams to incrementally deliver enhanced functionality based on an evolving understanding of user needs. For example, the Marketplace Lite App 2.0 continues to be iteratively improved based on user feedback and metrics.

5. **Choose a modern technology stack.** The Scalable Login System was built with industry standard open source software components commonly used by the private sector. The service is deployed in the public commercial cloud. These decisions enabled the team to build the service at a lower cost.

Modernizing the Immigration System at DHS

The Challenge

Every year, the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) processes millions of immigration requests. This system is mostly paper-based, consists of multiple forms, and results in long waiting periods for applicants who have little visibility into the status of their applications.

USCIS wanted to modernize the process. They wanted a streamlined experience that would allow applicants to identify which form was meant for their specific situation, and enable adjudicators to process applications more efficiently and effectively than on paper.

To achieve this goal, USCIS began a five-year engagement with a technology vendor to create the Electronic Immigration System (ELIS). The project ran into a host of issues: the project scope was too large, the proprietary technology adopted was too complex and inflexible, and releases happened years after the project began. The agency was heavily reliant on specific vendors and proprietary technologies that proved costly and difficult to customize to address USCIS' product requirements.

ELIS fell short of expectations and didn't meet user needs – so USCIS made the hard but correct decision to restart the project using a new management style and a new technical approach that took key plays from private industry.

In 2014, members of the USDS joined the USCIS team to help the agency implement these changes, and the USDS has provided ongoing support to the agency since then.

Project Impact Summary

- Every year, USCIS processes millions of immigration requests. Its multi-year project to modernize this process (the ELIS project) ran into a host of issues common in Federal Government IT projects, leading USCIS to restart the project.
- In 2014, USDS staff engineers, designers and product managers began working with USCIS to help it implement private sector IT management best practices including agile software development and continuous integration.
- In March 2015, following a November 2014 soft launch, USDS supported USCIS with the release of online filing and adjudication of the Form I-90, the application to replace permanent resident cards. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.

- In February 2015, USCIS partnered with 18F, private contractors, and USDS to launch myUSCIS, a new service to help applications and their representatives better navigate the immigration process.
- The Immigrant Fee payment launched in August 2015, enabling over 1.1 million applicants to make fee payments digitally.
- USCIS has adopted deployment approaches that allow it to release improvements to ELIS weekly, compared to the quarterly release schedule the project followed previously.
- Today, 25% of immigration applications are processed electronically and USDS continues to work with USCIS to increase this percentage.

The Solution

In restarting the project, USCIS leadership changed the way they did business.

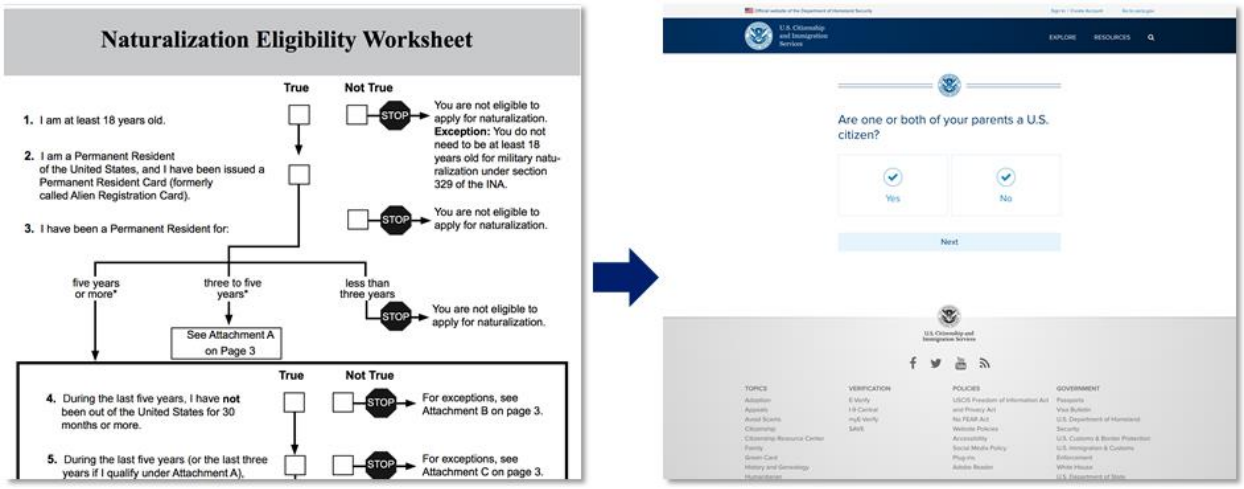
The team embraced an agile, iterative style of product development that allowed the agency to design, build and deploy functionality more quickly to respond to user needs. While the previous project had taken years before an initial launch, the new approach led to a beta release just one year after development began. Agency staff are now heavily involved in the day-to-day development effort, running stand-up meetings and increasing visibility across the team. Seasoned USDS product managers, engineers and designers partnered with the USCIS team to integrate these modern digital service practices.

In order for the team to effectively support this agile development style, USCIS had to change its approach to contracting. They engaged with multiple vendors instead of using one large contract with a single vendor. The teams worked together to deliver features, build and maintain the infrastructure for the service, and enable the continuous integration of new improvements into the production system. The contracts are designed to support frequent prototyping, refining of product requirements, and delivery of working software. Most of them give USCIS the flexibility to ramp up or down the number of development teams from each vendor based on that vendor's performance.

USCIS also conducted deep research on their customers that led them to re-imagine the end-to-end immigrant experience well beyond the core actions of filing and processing requests. They began to redesign the immigrant experience around people, not form numbers.

In partnership with 18F and private contractors, USCIS brought this vision to life by launching myUSCIS, a new service built to help applicants and their representatives.

myUSCIS allows visitors to determine which immigration options are available to them, with a search-driven, plain-language knowledge base of direct answers to common immigration questions. It also now allows immigrants to apply for naturalization, make fee payments, provide supporting evidence, and look up their case status online.



Finally, USCIS technical leaders also made important changes to the architecture of ELIS. The development team has adopted many modern software development practices drawn from the private sector, including the use of open source software components, flexible deployment environments, and real-time monitoring. The team also continuously integrates changes to the system, using modern deployment and testing processes and tools. USCIS is implementing the "DevOps" model, in which there is no separation between development and operations teams.

These improvements in software development practices, design and system architecture are making it easier for users to interact with our immigration system. The team has hit several important milestones, including the release of online filing and adjudication of the Form I-90 (application to replace permanent resident card). USCIS has also begun to electronically process applications for naturalization. USCIS will continue to bring more parts of the immigration process into the new digital system and improve its processes around design, high-quality delivery, and system monitoring and response.

USDS will remain involved with the project to assist with delivery, design and operations.

Success Criteria	Status
Increased percentage of immigration applications processed electronically	In progress. 25% of immigration applications are now processed electronically
Increased customer satisfaction rating over time	In progress. 92% of online I-90 filers (renewing or replacing their green cards) reported being satisfied with the experience.
Increase frequency of ELIS releases	Complete. ELIS releases new code weekly, up from previous quarterly releases

Milestones

- July 2014: A "pilot" USDS engagement prior to its official launch in August began with a “Discovery Sprint” focused on ELIS
- November 2014: ELIS2 I-90 Three-Day “Soft” Launch
- March 2015: ELIS2 I-90 Full Launch
- August 2015: Immigrant Fee payment launched
- April 2016: ELIS2 Naturalization Pre-processing Go-live Date

The Process and Lessons Learned

1. **Understand what people need.** The USDS team helped USCIS implement a user-centered design process to ensure that the delivery team understood what people need the service to offer. USDS coordinated and led visits to field offices and the National Benefit Center to conduct direct observation of application processing, giving insight into users' needs and experiences. This user research informed the design of the system. The team further refined these designs by getting adjudicator feedback on simple mockups of functionality, and testing early versions of the system with adjudicators.

2. **Build services using agile and iterative practices.** In the new system, USCIS chose two high-volume services and focused on rapidly digitizing them using an

agile development process. The Form I-90 application to replace a permanent resident card was first launched in November 2014, and USCIS Immigrant Fee Payment launched in August 2015. These services were rolled out in an incremental manner, and teams continue to deliver bug fixes and enhancements on a weekly basis. The teams collect feedback from end users and engage in regular usability testing to identify opportunities to improve efficiency and inform development of future product lines.

3. **Structure budgets and contracts to support delivery.** The USCIS CIO spearheaded an innovative contracting approach, which replaced a single large vendor with multiple contractors working together and competing for business. Each contractor provides cross-functional development teams that participate in the iterative product development process, working with federal product owners and project managers. Each vendor is evaluated based on its ability to rapidly deliver working software.

4. **Deploy services in a flexible hosting infrastructure.** USCIS chose to use a "public cloud" infrastructure service provider to host the service. This choice makes it easy and cost-effective for the team to provision, configure and adjust virtual computing resources as needed.

5. **Identify and empower product owners.** USCIS centralized the product development effort in its Office of Transformation Coordination, led by a single executive. This executive has identified product owners for each business line, who are each empowered and responsible for the digitization of that business line's product. Each product owner can prioritize work, advocate for users, and accept delivery of features from the contractor staff. USDS provided training and support to these product owners, and advocated for the creation of this product management structure.

6. **Implement robust monitoring and incident response.** USDS led an initiative to create a rapid response procedure for troubleshooting major incidents such as service outages. This procedure involves identifying "incident commanders" who are empowered to make quick decisions and the use of an alerting tool (currently PagerDuty) to coordinate incident response.

7. **Use "soft launches" to help identify issues prior to full release.** The USCIS team has incremental releases built into its process. For example, the ELIS2 external interface was opened to accept I-90 applications for 72 hours in November 2014. The applications received in this "soft launch" window were then processed using the new system, allowing USCIS to complete an end-to-end test

of the service with real data. The results of this test were used to refine the service prior to its full launch in February 2015.

8. **Rely on automated tests to increase development speed.** Good automated test coverage allows the team to verifiably demonstrate the system is working as intended, and speeds the development process by providing instant and reliable feedback to developers about how changes they have made to the system have impacted existing functionality. Working together, USDS engineers and contractor teams have increased the use of automated unit and integration tests.

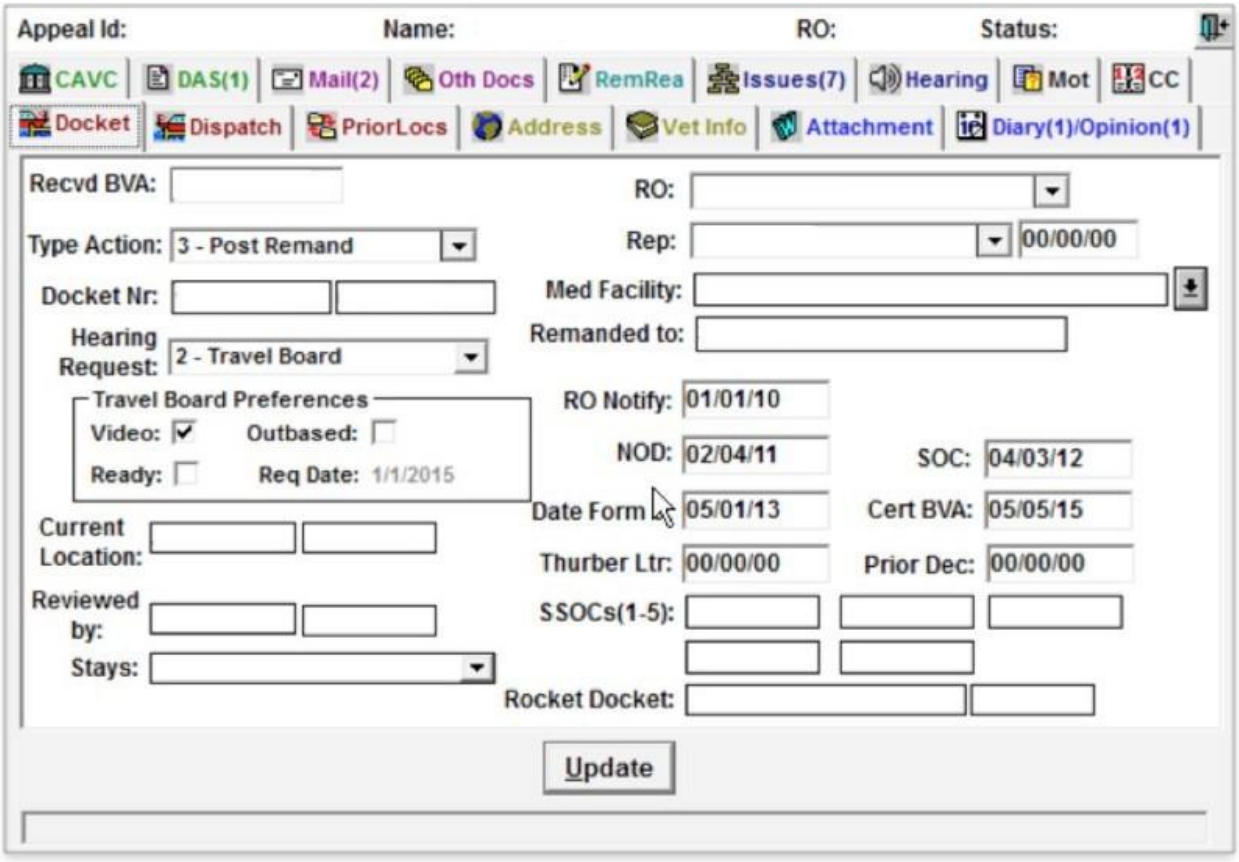
Streamlining VA Disability Claim Processing

The Challenge

When a veteran has a disease or injury related to service, he or she may file a claim for disability compensation for the service-connected disease or injury. These claims are filed with the Department of Veterans Affairs (VA) and can result in a grant, partial grant, or denial. If a veteran is unsatisfied with the outcome of his or her claim, he or she may file an appeal. Since 1996, the appeal rate has averaged 11 to 12 percent of all claims decisions.

Between FY 2010 and FY 2015, the Veterans Benefits Administration (VBA) completed more than 1 million claims annually, with nearly 1.4 million claims completed in FY 2015. As VA has increased claims decision output over the past 5 years, appeals volume has grown proportionately. Today, there are more than 450,000 pending appeals, and this number is expected to grow to 1 million by 2025 without legislative reform.

The current IT system used to track and process appeals at the Board of Veterans' Appeals and across the VA is more than 20 years old and is built on outdated infrastructure. It powers a variety of workflows essential to the appeals process across VA, but is difficult to use and hard to update, and it is straining under the increased volume of appeals. With such a large volume of paperless cases that travel across jurisdictions within the VA, from the local regional office level to the Board and back again, the VA needed an updated IT solution to ensure full and seamless accountability of all appeals as well as data integrity through integration of systems, increased automation, and reduced manual processes. VA recognized that the processes and technology underpinning the appeals system needed improvements, and began the Appeals Modernization initiative in 2014.



A screenshot from the current VA IT system used to track and process appeals

Project Impact Summary

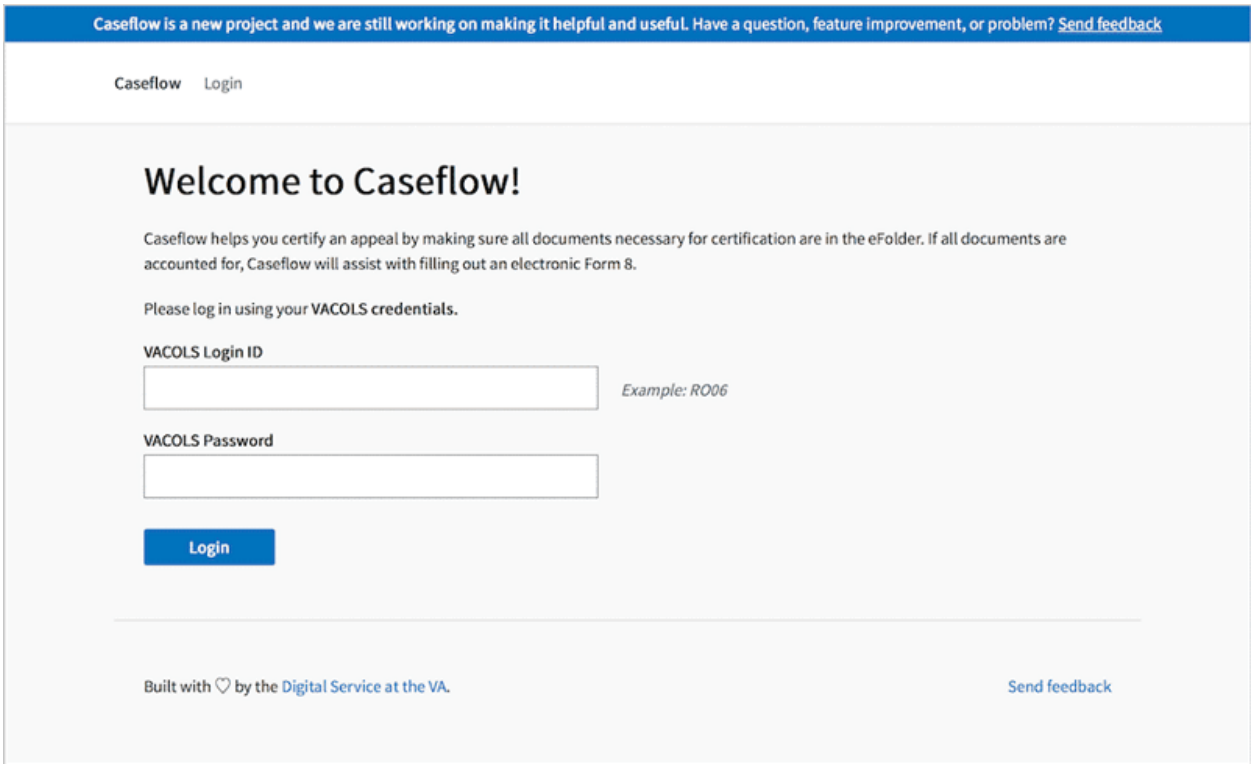
- The legacy IT system used to track and process appeals at the Board of Veterans' Appeals is more than 20 years old and is built on an outdated infrastructure.
- A team of three Digital Service at VA staff worked with the VBA beginning in June 2015 to design and implement a new Caseflow Certification tool to provide the Board with all of the information it needs to process an appeal.
- Digital Service at VA developed a script that discovered 2,172 appeals that had been incorrectly categorized and were in limbo. Without this script, appeals in this state may have remained unprocessed for an indefinite period of time.
- As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow Certification. The new tool was successfully rolled out as certification volume increased 34.1% from the year ago period.
- As of September 2016, Caseflow Certification handles 5,000+ certifications per month.

- Digital Service at VA awarded an agile contract on T4NG in September 2016, using a coding exercise to determine contractors' capabilities.
- With a new contract in place, the Caseflow team is growing to 30, including nine Digital Service at VA staff.
- In October 2016, Digital Service at VA began rolling out eFolder Express to the Office of General Counsel and the Records Management Center to improve the efficiency with which appeal documents can be retrieved, including for Privacy Act requests.

The Solution

The U.S. Digital Service at VA (DSVA) – the U.S. Digital Service's first agency digital service team – has worked closely with the Board of Veterans' Appeals to develop a new system that tracks and processes paperless appeals, called Caseflow. This system will have many user-facing web applications that map to existing workflows in the appeals process such as Certification, Activation, Review, and Dispatch. The team is using an iterative approach that will gradually replace small portions of the older system as new components are created, minimizing any disruption to existing business processes. In addition, the USDS modular approach enables quick updates and changes to Caseflow should there be any changes in legislation, regulation, or VA policy.

Caseflow Certification, released nationwide in April 2016, is the first component of the modernized system to be deployed. Caseflow Certification is a tool for VA employees to ensure that the Board has all of the information it needs to process the appeal, and that the data in the claims system — known as the Veterans Benefits Management System (VBMS) — matches the data in the appeals system, known as the Veteran Appeals Control and Locator System (VACOLS). Because many appeals that arrived at the Board contained manual data errors or were incomplete, providing VA employees at regional offices better tools to verify and reconcile key information using automated steps has been critical to optimizing accuracy and efficiency, and ensuring data integrity through system integration. Caseflow Certification also provides a simplified way for staff to generate a VA Form 8 – the Certification of Appeal – which is a required step in the appeal process. The tool automatically populates many fields of this form based on data in the system, reducing manual data entry to just a handful of questions. It also allows staff to file the form in the claims system with a single click, rather than requiring users to switch browser windows, navigate to the veteran’s case folder, and manually upload the form.



A screenshot from Caseflow.

In addition to the user-facing component, Caseflow Certification allowed the DSVA team to develop and run an important script that helps the Board identify pending appeals that may have been incorrectly categorized as paper transfers, when in fact the appeals were paperless. Without this step, the Board could be left waiting for a physical appeal to arrive at its facility when in fact none exists. Without the Caseflow Certification tool, appeals in this state could have remained unprocessed for an indefinite period. The DSVA team discovered 2,172 appeals in this state by running the script. This enabled the VA to proceed with processing these Veterans' appeals, and to take preventative measures to avoid the problem in the future. The DSVA continues to monitor the data to detect appeals that could end up in this state again.

As of September 2016, approximately 87.3% of all paperless appeals are now certified using Caseflow. The remaining appeals are certified using the legacy process, and represent edge case scenarios. The DSVA is working to incrementally improve the Caseflow Certification tool so it can be used in more of these uncommon scenarios. Throughout the rollout, DSVA promptly responded to feedback and issues reported by VA employees.

Success Criteria	Status
All appeals are certified using Caseflow	In progress. At present, 87.3% of paperless appeals are processed using Caseflow.

Milestones

- June 15, 2015: DSVA engagement began
- July-August 2015: Discovery Sprint
- March-April 2016: Caseflow Certification rollout to all VA regional offices
- September 1, 2016: Agile Contract awarded on T4NG with coding exercise
- October 2016: Rolled out eFolder Express to Office of General Counsel and Records Management Center

The Process and Lessons Learned

1. **Understand what people need.** The DSVA team visited the New York Regional Office to collect feedback on Caseflow Certification in October 2015. The team conducted five usability sessions, and used the feedback to improve the tool. The team visited again in December 2015 to gather additional feedback and verify the tool worked as intended in production. Additional usability tests were conducted in the St. Petersburg, Roanoke, Boise and Lincoln regional offices. Testing the service with actual users was critical for building a service that worked for veterans.

2. **Account for training materials and help desk support information.** Prior to rollout, the team needed to prepare training materials for staff who had to use Caseflow. Rather than creating a click-through slide presentation with quizzes, the DSVA decided to record a 5 minute screen share tutorial. Regional Offices provided positive feedback on this format, which they felt was short and specific. In addition to end-user training, the team had to prepare knowledgebase documents for the helpdesk staff who would field support requests from end users.

3. **Launch incrementally.** DSVA established a rollout schedule phased over a month. The team started off with the launch at the New York Regional Office whose employees were most familiar with the tool from the in-person usability

sessions. From there, DSVA launched in the other regional offices where it conducted remote usability testing. In each subsequent week the team rolled out the application to a larger and larger group of regional offices until it was deployed in all offices.

4. **Ensure application has appropriate monitoring.** The lack of robust application monitoring made it difficult to identify issues with the system. For example, the identity access management service used by the tool went down several times over the rollout period, preventing access to Caseflow. Better monitoring would have allowed the team to identify issues like this before they impacted end users.

5. **Improve automation.** Automation can help improve many aspects of the appeals process (and many similar case processing systems in government). For example, a VA employee shouldn't need to manually re-type information from one system into another system in order to create a form. But there are times in a case processing workflow where human judgment is required. Instead of attempting to account for every edge case, case management systems should automate the most common use-cases, eliminate redundant tasks, and empower staff to use their knowledge and expertise to navigate and resolve tricky edge cases when necessary.

Simplifying Veteran-facing Services with Vets.gov

The Challenge

Presently, Department of Veterans Affairs' (VA) digital services, such as obtaining a prescription refill, applying for healthcare benefits, checking the status of a claim, and accessing VA forms, are spread across hundreds of public-facing VA websites. Veterans must navigate disparate online systems, remember multiple user names and passwords, and contend with long pages of legalese to access benefits they have earned.

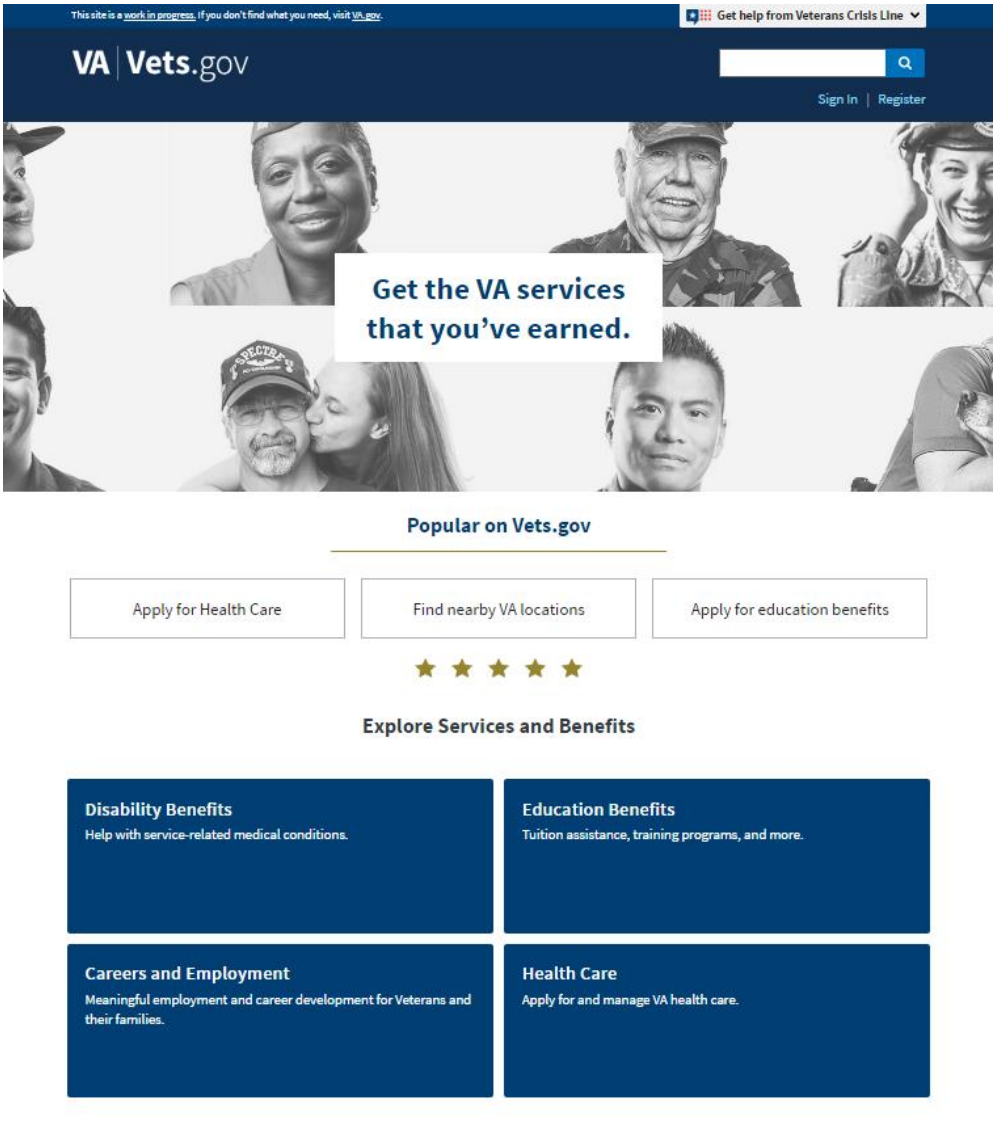
Many of the systems that power these services are outdated and provide a poor user experience. For example, the current digital 10-10EZ form to apply for healthcare was built as a fillable PDF, which requires Adobe Acrobat. The only browser that defaults to Acrobat for PDFs is Internet Explorer, so based on current browser usage, 70% of visitors saw an error message when they tried to apply. As a result, since 2012 only about 8% of all VA healthcare applications were submitted online.

Project Impact Summary

- Many of the systems that power VA’s digital services are outdated, and are spread across hundreds of public-facing VA websites.
- In November 2015, the Digital Service at VA launched Vets.gov, a mobile first, cloud-based platform that provides a new way for Veterans to discover, apply for, track, and manage their benefits.
- The initial Vets.gov website included plain language content for education and disability content and several tools: GI Bill Comparison Tool, Facility Location, and a Veteran feedback forum.
- Since then, the vets.gov team has launched 39 products, and reduced release cycle times from 90 days to 7 days.
- In June 2016, a new digital healthcare application was added to Vets.gov. In the first 60 days, 41,000 online submissions were received; an increase from a daily online submission average of 62 per day to more than 500 per day.
- VA is tracking to increase online health care applications from 10% (of 582,000 health care applications received by VA) in 2015 to 50% in 2017.
- In November 2016, the VA Digital Service team will launch several new features including: online application for education benefits, ability to check your disability claim status, prescription refills, secure messaging your health provider, and more.

The Solution

In November 2015, the VA launched Vets.gov, a new way for Veterans to discover, apply for, track, and manage their benefits. Instead of visiting numerous websites with multiple logins to have their benefits explained to them, Veterans told the USDS design team that they wanted to go to one site to get things done.



The Vets.gov homepage

Specific pieces of functionality planned include the most demanded health and benefits services, such as an accessible health care application that does not require specific software to complete. New functionality will also include claims and appeals statuses, as well as prescription refill services.

Design and development of vets.gov is led by the U.S. Digital Service at the VA (DSVA) – the first established U.S. Digital Service agency team. It is built with modern, open source tools and is hosted in the commercial cloud. The DSVA is using an iterative development process in which features are continually designed, tested, and integrated into vets.gov. Vets.gov is being built in the open, where Veterans can provide feedback and report bugs directly to the DSVA team, who quickly respond to comments.

Success Criteria	Status
Vets.gov website is available to the public.	Complete. Alpha version launched November 2015. Authority to Operate complete.
Launch digital healthcare application.	Complete. Vets.gov digital healthcare application launched June 2016.
100% of relevant content and front-end functions migrated from 514 existing public-facing VA websites.	In progress. Content related to disability benefits, education benefits, and careers and employment has been migrated to date.
Measurably improved Veteran experience.	In progress. The new online health care application has increased online submissions from 62 per day to more than 500 per day. Metrics collected will include bounce rates, page views, percentage of applications submitted online, volume of support requests to VA call centers.

Milestones

The initial vets.gov website was launched on November 11, 2015. It is a cloud-based platform with a modern technology stack. Immediate benefits and features included the following:

- Mobile-responsive website
- 508 compliance improvements

- GI Bill Comparison Tool
- Facility Locator
- Disability Benefit content rewritten in plain language
- Education Benefit content rewritten in plain language
- Feedback forum to collect Veteran feedback on the website

Since November, the team has been conducting ongoing research with Veterans and delivered additional content and features on the site, including employment services, the crisis hotline, and most recently the healthcare application.

On June 30, 2016, a new digital healthcare application was added to Vets.gov to enable Veterans to apply for healthcare online, solving the problems that prevented many Veterans from using the previous online application. As a result, the number of Veterans applying for health care online increased from 62 per day to over 500 per day. VA is now on track to increase the percentage of Veterans applying online from 10% in 2015 to over 50% in 2017.

Migration will continue throughout 2016, focusing on the highest demand Veteran services including functionality such as applying for healthcare and obtaining prescription refills.

The Process and Lessons Learned

1. **Understand what people need.** Vets.gov is being designed based on Veteran feedback. The vets.gov team works with Veterans regularly on research activities including usability testing, card sorting, and contextual interviews, using a combination of remote / in-person sessions and individual / group sessions.

2. **Build the service using agile and iterative practices.** Vets.gov is being iteratively developed, with new functionality released incrementally and refined based on feedback from Veterans. To manage this iterative process, the vets.gov team uses industry-standard techniques such as sprint planning and stand-up meetings for each vets.gov product team. These processes enable open communication and fast problem resolution. The whole team holds retrospectives every quarter to review progress and troubleshoot challenges.

3. **Engage stakeholders across the agency.** As a change management tool, the team opened bi-weekly vets.gov 101 briefing to all VA employees and stakeholders. To ensure leadership was fully engaged, the team had regular meetings with the Secretary and Deputy Secretary. The team was fully transparent in its planning and reporting by opening up the vets.gov roadmap to anyone at

the VA and offering status reports daily to anyone at the VA. Finally, weekly VA Change Management working sessions with communications leads and VA stakeholder meetings helped the team bring diverse players to a common understanding of the vision and goal to ensure success.

Providing Secure Access to IRS Taxpayer Information

The Challenge

Over 150 million taxpayers interact with the IRS each year. The IRS wants to offer taxpayers digital services such as online access to individual tax records and tax refund statuses. There is clear demand for these services from taxpayers – for example, the "Where's My Refund" online tool is one of the most popular Federal Government websites, with over 200 million requests in 2015. However, providing online taxpayer services is difficult due to the challenge of distinguishing a legitimate taxpayer from an identity thief who may try to steal information held by the IRS to commit fraud. IRS currently withstands more than one million attempts to maliciously access its systems each day.

One important IRS digital service is Get Transcript Online. The tool lets taxpayers access their official tax history, which can be needed for student loan applications, mortgage paperwork, or even filing the current year's returns. In May 2015, widespread unauthorized access of the tool forced IRS to take it offline. After analysis, IRS determined that bad actors had been using taxpayers' personal information stolen from data breaches outside the IRS to circumvent the tool's identity verification process. As a result, some taxpayer information was released to unauthorized users, who used the data to commit tax return fraud.

Creating a new authentication system that solves the difficult challenge of verifying the identity of individuals seeking to use IRS services was a top priority for the agency. Not only would this allow the IRS to restore access to the Get Transcript Online tool, but a method for securely identifying taxpayers is a prerequisite for many future digital services that the IRS is seeking to build for the American people.

One approach considered early in the Secure Access project was to add a "PIN in the mail" step to the user registration process, in which the IRS would mail an activation code to a taxpayer's physical address. The IRS was not satisfied with this solution because it wouldn't provide a better user experience than the default process of simply mailing tax transcripts directly to taxpayers that request them, a process which takes 5-10 days. The IRS wanted a solution that would allow taxpayers to get access to their own data in minutes, not days.

Project Impact Summary

- In May of 2015, the IRS removed the ability for millions of taxpayers to get online access their tax transcript because the "Get Transcript Online" service had been abused by unauthorized users.
- One option considered to secure the service would be to physically mail transcripts or account PIN numbers. However the IRS wanted a solution that could be completed in minutes, not days.
- A team of three USDS personnel worked with IRS beginning in October 2015 to help design and implement a new Secure Access online process.
- With the help of the USDS team, IRS executed a controlled launch in which the new service was tested with small groups of real users prior to full launch. The team also implemented fine-grained error-tracking and log monitoring. With this approach, USDS helped IRS achieve a 4x reduction in the error rate prior to full launch.
- The new Secure Access process takes an average of 12 minutes for users to complete, compared to the 5-10 calendar day wait for mailed transcripts without Secure Access.
- "Get Transcript Online" was returned to service for all taxpayers using the new Secure Access process in June 2016.
- As of August 22, 2016, taxpayers have accessed over 2.7 million transcripts using the online Secure Access process.
- IRS plans to re-use the Secure Access process for four additional services in IRS' e-Services suite.

The Solution

Recognizing the importance of secure online access, the IRS asked to partner with experts from the USDS in determining how to strengthen their authentication protocols while remaining convenient for taxpayers. Together USDS and IRS outlined the characteristics of a tool called "Secure Access": a user verification process using strong identity proofing and two-factor authentication in line with both industry best practices and federal standards from OMB and NIST.

The new system adheres to the "Level 3" standards of Electronic Authentication Level of Assurance, as defined by NIST in SP 800-63-2. This level of assurance requires an individual to demonstrate control over a physical object (i.e. "something you have") in addition to demonstrating knowledge of personal information such as name, birth date and social security number (i.e. "something you know"). The old system adhered to

LOA2, which allowed access to the system using personal information as well as knowledge-based multiple choice questions. This level of assurance proved insufficient, because some of the personal information used to verify users' identities in this approach had already been compromised in various data breaches from sources other than the IRS.

Using Secure Access to protect sensitive applications like Get Transcript Online would enable taxpayers to have convenient, real-time access to their transcripts without making that information vulnerable to automated fraudulent attacks. Working side by side with the agency, USDS helped IRS deliver the Secure Access project following principles from the Digital Services Playbook. These proven approaches enabled the IRS to efficiently deliver the Secure Access project in a timely manner. In June of 2016, the IRS launched Secure Access and brought Get Transcript Online back into service.

Success Criteria	Status
Restore online access to tax records in a manner that is secure against automated attacks (implementation of the NIST Level of Assurance Level 3 standard)	Complete. Service launched in June 2016. As of August 22, 2016 taxpayers have accessed over 2.7 million transcripts.
Build an account creation process that takes less than 15 minutes for a user to complete.	Complete. Account creation takes an average of 12 minutes, vs. 5-10 days for mailed transcripts or PIN numbers.
Implement error tracking and log monitoring. Collect and report daily business metrics.	Complete. Daily statistics on attempts, pass rates, error rates and overall traffic are collected and disseminated. Error tracking and log monitoring implemented. Phased launch strategy resulted in fourfold reduction in error rate.
Secure Access process used for at least one additional IRS service in addition to Get Transcript Online.	Complete. Secure Access is now used for the "Get an Identity Protection PIN" service in addition to Get Transcript Online. IRS also plans to implement Secure Access for four additional services in IRS' e-Services suite (Registration Services, e-File Application, Transcript Delivery, and TIN Matching).

Milestones

- October 2015: Discovery Sprint completed
- November 2015: Project start date
- February 2016: Secure Access protocol code completed
- March 2016: Internal employee test
- May 2016: Service launched to production, beginning controlled phase-in approach
- June 2016: Service launched to all users

The Process and Lessons Learned

1. **Assign one leader.** The IRS recognized the need for a single executive to help provide consistent oversight over all authentication and authorization needs across the many IRS functions and channels. They created the Identity Assurance Office, led by a senior IRS executive with experience working with both business and information technology groups. USDS worked side by side with this executive, helping clarify the business, product, process, and technical decisions that come with the responsibility of meeting user demands. USDS also worked with partners at OMB and NIST to get relevant background information that would help this leader make decisions that would meet federal standards while also meeting both user and business needs.

2. **Understand what people need and design a simple and intuitive service.** USDS worked with the IRS team to maintain constant focus on taxpayer needs. At the beginning of the project, USDS gathered input from the United Kingdom's Government Digital Service to inform early directions and learn from this organization's hard-won experience. One of the key insights from the U.K. team proved particularly valuable. The U.K. team learned it was important to set user expectations about how the authentication process would work up front, and to provide graceful alternatives if the user cannot or does not wish to continue with the online authentication process.

   USDS worked with the IRS to create draft user flows and tested them with users on a weekly basis. USDS improved the navigation, flow and messaging based on these tests. For example, an early prototype confused taxpayers by stating that authentication would require a "Credit card or auto loan, mortgage, home equity loan account number." In usability tests, the team learned that taxpayers thought they needed the account number for the credit card, not just the last eight digits of the credit card itself. The team changed the wording to be clearer. The IRS will

continue to use this iterative design process to help determine which features and fixes should be prioritized.

3. **Build the service using agile and iterative practices.** In addition to the iterative design process described above, at the suggestion of the USDS, the IRS used a phased launch process to test and refine the Secure Access protocol before its full launch. Initially, the agency limited access to the authentication system to only IRS employees. This controlled test allowed the team to get end-to-end user data that accelerated debugging and improvements.

4. **The USDS worked together with developers and business analysts to understand how users were getting stuck in order to improve the process.** An example of an issue that was discovered and fixed in this controlled launch was in a data entry field. When users were prompted to enter their account number, some users included the "#" character when typing the number. This would generate an error message that explained the "input was too long," confusing users. This problem did not surface in internal quality assurance testing, and would not have been discovered without letting real users interact with the system prior to full launch. The team fixed the problem and redeployed the improved code to another cohort of internal users. After this internal test, the IRS used a public beta period where the improved Get Transcript Online service was offered to a small percentage of public visitors to the IRS website. This beta period allowed the team to fix even more issues. This iterative process was used to identify and fix many subtle errors and points of confusion prior to full launch.

5. **Use data to drive decisions.** Collecting good data on how users were interacting with the system was a key to success. With USDS assistance, the IRS developers implemented fine-grained error codes and log monitoring. With this data, the team could categorize bugs and list the most common errors, allowing the team to prioritize its efforts. In one such case, a bug that resulted in a small number of users in the public beta test being unable to register was identified and eliminated. In this case, USDS engineers examined the code and speculated that an input validation filter on one of the field items had been accidentally set too strictly, rejecting some valid inputs. An IRS developer used the error monitoring data to identify that the error was highly correlated with specific versions of the Firefox web browser. With these insights, the team was able to identify the root cause of the error and deploy a fix before the tool's public announcement, saving hundreds of users a day from having the same issue.

   Between the initial deployment of the Secure Access protocol and the full public launch, iterative development coupled with good monitoring allowed the IRS to

achieve a fourfold drop in the error rate. The agency will continue to monitor errors and prioritize effort based on this data.

Improving the Visa Processing System at Department of State

The Challenge

The Department of State (State) protects the lives and interests of U.S. citizens overseas and strengthens the security of U.S. borders through the vigilant adjudication of visa and passport applications. State provides a range of services to U.S. citizens and foreign nationals, including issuance of U.S. passports and Consular Reports of Birth and Death Abroad and adjudication of nonimmigrant and immigrant visa applications. These processes largely are conducted through a collection of custom applications that depend on a system called the Consular Consolidated Database (CCD).

Many government systems, including the CCD, were designed at a time before most modern technologies to support distributed data processing were available. As a result, CCD's technical approach – innovative at the time it was implemented – deviates from what are now industry best practices. Over time, development focused on adding new features rather than modifying the underlying platforms and tools.

The integration of various components made the CCD progressively more complex. As a result, it became more difficult to ensure new features were integrated in a high-quality, easily maintainable manner. As demand increased, some tools were not able to be improved upon in a timely fashion.

Project Impact Summary

- In June 2016, the USDS team began discovery work around how to improve the visa application process. The team honed in on better ways to update applicants and petitioners on case status by making adjustments to a tool built in 2012.
- Over the past year, the CEAC Visa Status Check site received over 3 million visits per month from users ranging from petitioners in the United States to applicants across the world.
- The National Visa Center, a visa application processing center run by the Department of State, receives approximately 9,000 phone calls a day. The vast majority of those calls are about a visa applicant's case status.
- The USDS team, in partnership with the Bureau of Consular Affairs, is in the process of engineering improvements to the tool that will show users better

information about their case status and how to advance to the next stage of the application process.

- The USDS team performed robust user testing of the new status tool and tested how improved information using plain language may help cases move more quickly through the appropriate parts of the process.
- The status tool will launch soon. We will measure the impact of the tool against several metrics, including how it impacts the National Visa Center's call volume.

The Solution

USDS worked closely with State's Bureau of Consular Affairs' Office of Consular Systems and Technology (CST), which supports, develops, and maintains the technology that enables a global network of consular systems to support U.S. consulates and embassies, domestic visa processing centers, and domestic passport processing agencies and centers. CST already had a number of viable plans to improve overarching stability of the CCD and related applications, but attempts to execute these plans had been stymied by the system's complexity. USDS served as technical consultants, both vetting possible solutions and advising on industry best practices and as an empowering authority facilitating communication across divisions and organizations.

Success Criteria	Status
Standardize software development processes and tooling, enabling the Federal Government to have better visibility into contractor-developed custom software.	Completed. Established central source control repositories on a unified source control system. Completed a pilot that has improved developer workflows and allowed greater oversight into how code is being developed.
Transition how information is batched and sent to partner agencies to ensure there are no artificially created backlogs.	Completed. Changes made from both ends have been implemented and information is more efficiently transferred between agencies.
Immigration process and status is clear and comprehensible to applicants.	Ongoing. USDS team is currently implementing improvements to an existing tool that should more clearly communicate case status to applicants.

Milestones

- December 2015: USDS began engagement to improve information security of various State applications.
- February 2016: USDS began exploration of what kind of developer tools were needed within State to improve engineering practices.
- March 2016: State received USDS recommendations for improved developer tools, including usage of version control software.
- April 2016: USDS began assisting a State vendor with implementation of a version control software pilot.
- April 2016: USDS began discovery work on how to improve how State transmits information for Security Advisory Opinions with partner agencies.
- June 2016: USDS began determining ways to improve how visa status information is shared with applicants, petitioners, and their agents.
- June 2016: Technical implementation of the Security Advisory Opinion data sharing process began.
- July 2016: Technical implementation of improvements to visa status check tool began.
- September 2016: Completion of the technical and business process changes for the Security Advisory Opinion data sharing process.
- September 2016: USDS completed work on a pilot that saw a number of contractors using modern software development tools in the form of version control software.

The Process and Lessons Learned

1. **Working with and Empowering the Agency:** State identified a number of areas where it could improve its information security. USDS provided assistance in the form of consultation on system remediation and coordination of implementation. USDS also worked closely with teams within State to identify how to prioritize various kinds of remediation that needed to be implemented and how to rank ongoing concerns. Using these techniques, State has markedly improved its defensive posture.

2. **Breaking Agency Silos to Solve Problems Together:** In many cases both the technical expertise and the most appropriate solution were already present within the organization. However, in an agency the size of State it is sometimes difficult to convene these groups and share solutions to senior leadership and across the agency. USDS conducted extensive site visits to bring various branches and contractor groups across State together, and with State leadership's help was able to create cross-team collaboration that sped up the development and deployment of solutions. The project to modernize developers' tools, for

example, is a collaboration between multiple divisions within CA/CST: Configuration Control, Systems Engineering and Integration, and Service, Systems and Operations.

3. **Technical Vetting and Evaluation:** USDS provided State program and project managers with objective technical advice. This gave State better accountability and communication among contractors. Since problems were often spread over applications and systems governed by several contracts, government managers heard different technical explanations. USDS engaged in several “fact finding missions,” allowing State to use this information to prioritize tasks effectively.

4. **Embrace pilots:** Pilots are great opportunities to perform experiments in a contained, structured way. The ability to experiment is essential when bringing on new tools, services, or methodologies. It's not clear which will work best in a given environment, so experimentation is essential to bringing new tools, services, and methodologies to an organization. Knowing that the results will be used to determine if a pilot will continue helps stakeholders embrace new methods of doing things.

5. **Test early and often:** Manual and automated testing are essential parts of the software development process. Increasing your test coverage makes it easier to deploy a tool or functionality quickly and securely. We are hopeful that by working with stakeholders and contractor teams, we can improve the testing culture for how Department software is developed.

Helping CMS Implement Congressionally Mandated Medicare Payment Changes

The Challenge

In April 2015, Congress passed the Medicare Access & CHIP Reauthorization Act of 2015 (MACRA), changing the way Medicare pays doctors for services rendered to patients enrolled in the Medicare program. The act implements changes designed to reward health care providers for giving better care, not just more care. These changes will impact a large percentage of Medicare Part B payments, and the Centers for Medicare & Medicaid Services (CMS) seeks to ensure the transition from the current payment program to the new system is simple, clear, and effective.

Project Impact Summary

- Implementation of the Medicare Access and Chip Reauthorization Act of 2015 required a transition of payment programs that would impact a large percentage of Medicare payments to doctors.
- CMS engaged the USDS team to draw on best practices from other large program implementations.
- CMS created an integrated project team that combines policy and operations, and uses agile methodologies and other modern technology practices.
- The development team has employed user research, user need analysis and constant iterative feedback loops with users to ensure transition success.
- On October 14, USDS helped CMS released the Final Rule for implementing MACRA concurrently with a plain language website describing the rule. The website serves two purposes: first, to help clinicians and their partners easily understand how MACRA impacts them and, second, to serve as a single entry point for clinician interaction with the program in the future.
- The MACRA implementation is still on-going and iterative development will continue throughout 2017.

The Solution

MACRA implementation is an important priority at CMS. USDS is helping CMS take an implementation approach that draws best practices learned from implementing other large programs, including HealthCare.gov and the adoption of the 10th revision of the

International Statistical Classification of Diseases and Related Health Problems (ICD-10) standard. Key priorities include widespread user research and user needs analysis, an integrated project team across CMS responsible for program delivery from policy to operations, a tight iterative feedback loop with users to inform program design and ensure that it is clear and accessible, and incorporation of modern technology best practices.

Success Criteria	Status
Contracts for key elements of MACRA implementation are agile and responsive to evolving program needs.	In progress. CMS has successfully used agile acquisition practices across most of the contracts for the MACRA program.
Project team is integrated and running off of a shared roadmap for execution, including user research, policy, procurement, operations, technology, and analytics.	In progress. CMS has identified a product owner for MACRA implementation. CMS staff and contractors work on an integrated team.
Modern technology development best practices are being used in the creation of program infrastructure.	In progress. USDS assisting CMS staff and contractors to implement best practices in design and engineering.

Milestones

- February 2016: USDS Discovery Sprint/Project Started
- May 2016: Development work started
- October 2016: Final Rule with Comment and website concurrently launched

The Process and Lessons Learned

1. **Go where the work is.** The USDS team has pushed for extensive collaboration and information sharing between the USDS, CMS, and its contractor teams. The USDS team works alongside CMS staff and contractors on an integrated team at least four days a week in a shared space to facilitate this goal.

2. **Engage agency leaders and policymakers in the process.** The USDS team works hand-in-hand with CMS leadership on the program. The team is helping to ensure that implementation details, technical trade-offs, and operational complexity are communicated effectively to the whole team, including those writing policy.

3. **Identify a product owner.** CMS identified a single product owner for the implementation of the law, which has facilitated faster decision making.

4. **Provide contracting officers with agile acquisition training.** The CMS team was aware of agile acquisition practices, and their ability to implement agile contracts was significantly helped because one CMS contracting officer had already gone through the USDS agile acquisition training program. CMS has successfully utilized agile acquisition practices across most of the contracts for the MACRA program. The head of the division has further requested more training in agile contracting for the entire team.

Reducing Inefficiency in the Refugee Admission Process

The Challenge

In Fiscal Year 2016, President Obama set a ceiling of admitting 85,000 refugees into the United States. This represented a 15,000 person increase over the previous fiscal year's ceiling, and this increase depended upon improving the efficiency of the refugee admissions process.

One of the most impactful improvements was the introduction of the digital approval process for refugee applications. Previously, Department of Homeland Security (DHS) officers were only able to approve refugee registration forms using an ink approval stamp in the field where the refugee file is physically located. 57% of cases are finalized on a different day than the DHS field interview. In many of these cases the requirement for an ink approval stamp added an unnecessary delay of up to eight weeks after all security checks had been completed, as cases waited for a DHS officer to travel back to the field location where the file was located to stamp it approved.

Project Impact Summary

- In December 2015, USDS, the State Department, and the Department of Homeland Security established an interagency Refugee Coordination Center (RCC) staffed with representatives from each agency.
- The RCC began working on a prototype for digital approval of cases in January 2016 and launched the product for DHS use in June 2016.
- By September 30, 2016, 11,571 individuals had been digitally-approved, helping the Administration meet its refugee admissions goals while maintaining integrity in the process. Furthermore, the digital approval process codified rigorous security standards, granted DHS flexibility of when and where it can spend time doing administrative work, and saved the Department of State's Resettlement Support Centers time and money by eliminating the need to prepare and ship case files for ink approval stamping.
- State Department Resettlement Support Centers (RSCs) processing these cases stated that the following amounts of time were reduced in the admissions process as a result of the launch of the digital approval process: Bangkok: 1-2 months; Malaysia: 1-2 months; Middle East and North Africa: 1-6 weeks; South Asia: 15 days; Latin America: 15 days; Africa: 12 days.

The Solution

The digital approval process enables DHS officers to digitally-approve a refugee registration form without having to physically travel to apply an ink stamp on paper. The solution was created by granting DHS editing rights to the State Department's refugee case management system for the first time. Filters ensure that only cases ready to be approved appear for DHS to digitally approve.

In order to convert the manual process into a digital process, the RCC worked with DHS officers to convert all of the manual steps to approve a case into the new digital approval feature. These included:

Checking security statuses

In the manual process, DHS officers are required to physically review a security report for each individual on a case and annotate the page attesting that they have reviewed each page. In this digital approval process, DHS officers electronically affirm they have reviewed all security statuses and the case file, which then enables them to click the digital approval button.

Updating the hard copy form

In the manual process, DHS officers have a paper form that is a history of all actions made on a case. In the digital process, once a digital stamp is applied, the system automatically generates a new digital file for the case, including the time and date the case was digitally-approved, and is included in the case's physical file by the State Department.

Approving the I-590

In the manual process, DHS officers physically approve a refugee registration form (Form I-590) by applying an ink stamp to the approval block on the form. In the digital process, DHS officers click "stamped approved" and the system securely and automatically-generates an individual-level approval page with the time stamp and name of the approving DHS officer. The RSC staples this file to the front of the refugee form, which Customs and Border Protection reviews upon the refugee’s arrival at a port of entry in the United States.

Approval Letter

In the manual process, once a case is ready for approval DHS officers initial an approval letter. State Department Resettlement Support Centers then date the letter before

scanning it and then delivering to the refugee. In the digital process, the system automatically-generates an approval letter with the approving officer's initials and the time stamp when the case was approved, and it is automatically-saved in the case's digital file. The Resettlement Support Centers print and deliver the approval letters to the refugee.

The Role of the RCC

In addition to these process modernizations, USDS assisted with data modeling to predict the number of people who would benefit from digital approvals in order to justify dedicating engineers' time to develop this feature. USDS also designed the system requirements, created prototypes, and coordinated agency-wide approvals for the project. USDS then worked with State Department engineers to develop the new features, and with DHS officers to test the features prior to launch. USDS assisted with the phased roll-out of the digital feature, including training of DHS officers and development of Standard Operating Procedures (SOPs). Finally, USDS ensured that USCIS notified all stakeholders within DHS to prepare components for these changes prior to the first digitally-approved cases arriving in the United States.

Success Criteria	Status
Reduce the time between the date a case is ready for approval and the date it is approved to under two weeks.	On track. In August 2016, of all cases that were digitally-approved, 74% were approved in five days or less and 56% in two days or less. Of the 124 cases that took more than 15 days to digitally approve, 77% did not need to travel until January 2017 or later.
Reach 8,000 individuals approved digitally before the end of the fiscal year.	Complete. 11,571 individuals were digitally-approved by the end of the fiscal year.
Ensure at least 20 officers were part of the digital approval pilot.	Complete. By the end of the pilot, more than 60 officers were trained and had permission to use the digital approval process.

Milestones

- January 2016: Began prototyping and requirements gathering for the digital stamp

- March 2016: Finalized all data analysis, cost benefit analysis, completed requirements
- May and June 2016: State Department engineering team developed digital approval feature
- June 2016: Conducted user testing and fixed bugs in the system
- June 2016: Digital approval process launched
- September 30: Digital approval process pilot ends and full roll-out began

The Process and Lessons Learned

1. **Engage stakeholders across the agency and collaborate with subject matter experts.** Engaging stakeholders across the agency and working with civil servants who are subject matter experts was essential for the success of this project. In this case, the concept of digitally processing cases had previously been identified by individuals at DHS as an opportunity to increase efficiency. Identifying and collaborating with these individuals allowed USDS to make progress faster.

2. **Keep the scope narrow for the minimally viable product (MVP).** Despite pressure to expand the scope of the MVP that was prototyped, development remained focused on the most critical features for refugee officers and refugees. Throughout the development process, USDS focused on core user needs, replicating the existing physical process into a digital experience. This narrow focus ensured that work flows would remain largely unchanged for refugee officers.

3. **Understand users' needs by testing with actual users.** The digital approval process was built with input from internal users to ensure their feedback was understood and addressed prior to launch. While quality assurance testing by Department of State engineers was critical, USDS' time spent with DHS end users was important for uncovering a variety of issues that would not have been found through engineering team testing alone.

4. **Rely on pilots and build up to a successful launch.** USDS relied on an initial pilot period (from June 24th through September 30th) with limited users (at first only one user and by the end more than 60) to identify any new glitches. Additionally, USDS worked with DHS to develop Standard Operating Procedures and video, teleconference, and in-person trainings to ensure ease of use and clear understanding of the new digital process. Once the digital approval process was judged to be successful and stable with the small pilot group, it was rolled

out more broadly to additional users. There was unanimous support to roll out the digital approval process to all trained and eligible users in Fiscal Year 2017.

Helping Students Make More Informed College Choices at Department of Education

The Challenge

For students, higher education may be the single most important investment they can make in their futures to ensure they have the knowledge and skills needed to compete in an increasingly global marketplace. College is the surest path to becoming part of America's middle class and for this reason, selecting a college is an incredibly important decision for many people. But, many potential college students and their families do not have the advisors or resources to help them find a college that will serve them well.

With college costs and student debt on the rise, the choices that American families make when searching for and selecting a college have never been more important. Yet, students and the organizations that serve them struggle to find clear, reliable, and comparable data on critical questions of college affordability and value, such as whether they are likely to graduate, find middle-class jobs, and repay their loans. At a time when America needs colleges to focus on ensuring affordability and supporting all students who enroll, many of the existing college rankings instead reward schools for spending more money and rejecting more students. Additionally, college leaders and state policymakers who seek to improve institutions' performance often lack reliable ways to determine how well their schools are serving students.

To address this challenge, the Department of Education sought to redesign the College Scorecard.

Project Impact Summary

- The USDS team at the Department of Education, with help from 18F, launched the College Scorecard to help students and their families make more informed choices about where to go to school.
- The Scorecard makes comprehensive data on college costs, graduation rates, graduate debt, repayment rates, and post-college earnings accessible to help students choose a school based on access, affordability and outcomes.
- The project drew on hundreds of interviews with students, parents and guidance counselors to ensure that the product would fit their needs.

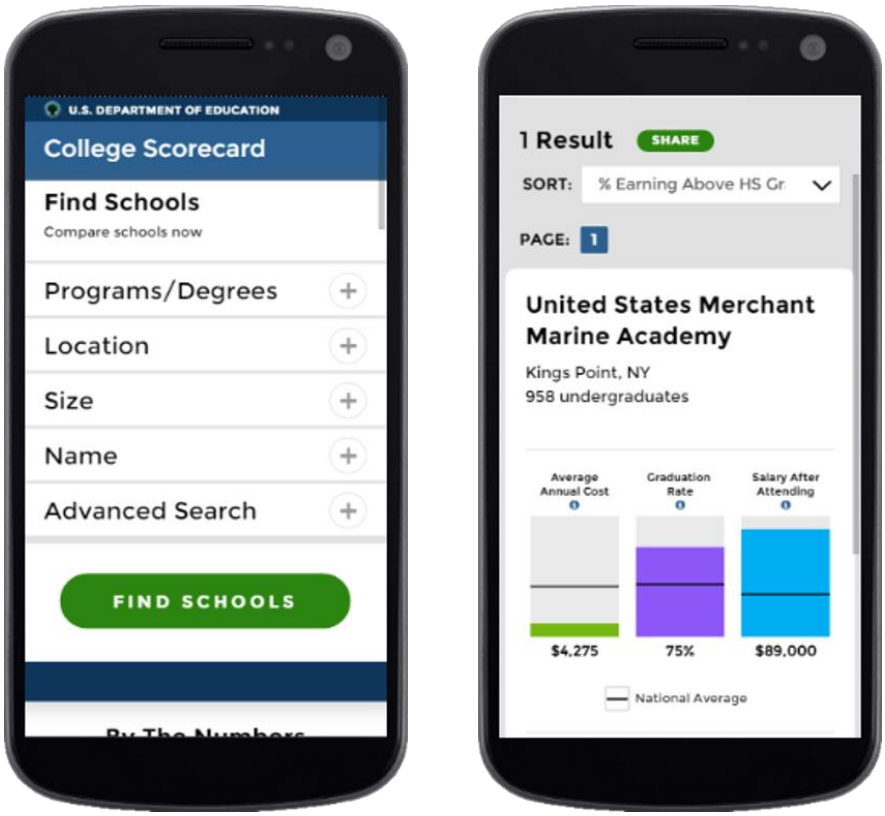
- In its first two weeks, College Scorecard attracted over 850,000 unique users, a major uptick from the 160,000 who used the prior version of the tool the entire year before.
- The project opened the data to the public and made an API available specifically for third-party developers to build more applications to help students and policymakers. More than a dozen organizations have built new tools using this data.
- Google has now integrated College Scorecard data so that it shows up front and center in the results of hundreds of millions of education-related searches.

The Solution

The new College Scorecard was redesigned with direct input from students, families, and their advisers to provide the clearest, most accessible, and most reliable national data on college costs, graduation rates, and post-college earnings. This new College Scorecard can empower Americans to rate colleges based on what matters most to them; enable policymakers and the public to highlight colleges that are serving students of all backgrounds well; and focus greater attention on making a quality, affordable education within reach. The new tool for assessing college choices, with the help of technology and open data, makes it possible for anyone—a student, a school, a policymaker, or a researcher—to evaluate an institution on the factors that matter most to them.

The public can now access the most reliable and comprehensive data on students' outcomes at specific colleges, including former students' earnings, graduates' student debt, and borrowers' repayment rates. This data is published through an open application programming interface (API), enabling researchers, policymakers, and developers to customize their own analyses of college performance more quickly and easily.

More than a dozen organizations are using this data to build new tools. For example, Scholar Match, Propublica, and College Abacus—three college search resources—are using the new, unique data to help students search for, compare, and develop a list of colleges based on the outcomes data that the Department of Education made available for the first time through an API. InsideTrack, comprised of a team of coaches and consultants working to improve student outcomes by helping students find the institutions that are right for them, uses the data to develop and implement effective student-centered initiatives.



The College Scorecard

The Department of Education plans to continue releasing new College Scorecard data and promoting use of these new access, affordability and outcome metrics.

Success Criteria

Success Criteria	Status
Engage a diverse set of students and their supporters, especially high-need, low-income and first-generation college-goers.	Ongoing. In the first two weeks the Scorecard was launched, it was accessed by 850,000 users. The previous version of the tool received 160,000 total users in the previous year.
Educate the marketplace and shift focus to key outcome metrics and institutional performance	Ongoing. External organizations and third party developers are making use of this new data in their tools and research.

Success Criteria	Status
Enable more informed college matching	Ongoing. As of September 2016, 1.5 million unique users have accessed the tool. The previous version of the tool received 160,000 unique views a year.
Foster continuous improvement	Ongoing. New data was released to the Scorecard in September 2016. All Scorecard information is now appears in search results for colleges.

Milestones

- April 2015: Project Start Date.
- July 2015: Code Start Date.
- September 2015: Go-Live Date.
- May 2016: USDS Project End Date.
- September 2016: New data released to Scorecard. All data indexed and searchable.

The Process and Lessons Learned

- **Understand what people need.** USDS, Ed, and 18F built College Scorecard by working with users at every stage of the project to find out how they made decisions about college. The team met with students (both high school and adult), parents, guidance counselors and advisors, open data users, and people who wrote to the President about their college search experiences. Long before the first line of software code was written, the team was working with students, testing paper prototypes to make sure they were as easy-to-use as possible.

Getting feedback on a paper prototype of the new College Scorecard.

- **Build services using agile and iterative processes.** The Department of Education built the College Scorecard using agile development methodology. To deliver the right product — what students actually need — as efficiently as possible, the team built the new College Scorecard using an approach that allowed the team to work in short iterations, and to test, scale, and design the tool with a process that could adapt to changes in technology and user needs. The team maintained a project rhythm of two week iterations, with daily stand up meetings to coordinate progress.

- **Run a developer beta.** USDS ran a beta specifically for developers — giving them a chance to test the data and documentation and flag opportunities to make it even easier to use. The feedback from the developers made it possible to release the data in a way that led to easy re-use by third parties.

- **Launch a minimum viable product (MVP).** The team focused on launching a MVP, building the right products to meet customer needs as efficiently as possible. This approach allowed the project to launch with less than 3 months of development time. The team built the project mobile-first and focused on the most critical feature set and information that each user type advocated for.

- **Release open data, and build services using the same APIs offered to the public.** Rather than focusing solely on creating a user-facing website, the team

also created documentation for, and released, open data for over 7,300 colleges and universities, going back 18 years. This made it possible for third-parties to incorporate the data into their own products and tools, increasing the chance that the information makes it to users wherever and whenever they might be looking for it.

To make it easier for third parties to integrate this data, Department of Education published an API. This API serves both as the engine for the College Scorecard itself as well as a source for external software developers or researchers who want to use the data in their own digital products. The College Scorecard effort is one of the first government digital services that not only releases open data, but also builds a user-facing tool on top of the very same API it provides to the public. This is a common practice used by American's best technology companies.

Modernizing the Department of Defense Travel System

The Challenge

The Defense Travel System (DTS) provides travel for all Department of Defense (DoD) employees (excluding permanent changes of station). While the DTS does provide end-to-end travel and expense functionality, the antiquated system provides a poor user experience and limited reporting capability. The system has long been a pain point for DoD travelers and officials, and has been scrutinized by lawmakers and auditors. For example, after the Government Accountability Office determined that DoD had overestimated savings for DTS and failed to fix implementation problems with the system nearly a decade ago, DTS added fees for the user and prevented travelers from quickly making changes to their reservations. Lawmakers have required the DoD to improve Defense travel through the creation of the Defense Travel Management Office (DTMO) and providing them with the Defense Travel Pilot Authority to find ways to improve the system and agreements that govern Defense travel.

Currently, the Department of Defense's travel spend is over $8.7 billion per year. Of this spend, $3.5 billion is handled through the DTS, with a per-transaction cost around $10. In addition, there are over 1600 pages of DoD travel regulations. Despite this, about 100,000 unique users access DTS daily, according to the DoD website.

The complexity of the Joint Travel Regulations imposes a challenge for standard DoD users, as well as Authorizing Officials who administer and authorize travel. Many of the policies make it difficult to apply commercial best practices to the system. For example, the policy precludes the integration of industry-standard features like restricted fares, which could ultimately lead to higher cost savings across the department.

Project Impact Summary

- The Department of Defense has long needed to improve the costly and cumbersome system used to book, expense, and manage travel for its employees.
- In March 2015, the Digital Service team at the DoD started working with agency staff to identify a new, commercial tool to better manage travel, and agreed to oversee a pilot test of the new system.
- At the same time, DoD worked to simplify its complex travel policy, with an eye toward saving millions of dollars and delivering a better user experience.

- In June 2016, the new software-as-a-service travel tool and streamlined policy were in place, and a pilot opened for “basic travelers.” Both are still being refined.
- This project demonstrates the potential of pairing policy development with technology implementation to produce more efficient outcomes, and reinforces the principle that using commercial software when minimal customization is required can save the Federal Government significant time and money.

The Solution

To reduce costs and improve the customer experience, DoD is seeking to modernize its travel system with a commercial software-as-a-service (SaaS) product. At the same time, DoD has committed to simplifying the travel policy under the Joint Travel Regulation (JTR). These changes have the potential to save hundreds of millions of dollars per year and improve satisfaction of Defense travel customers. The Deputy Secretary of Defense has directed the relevant human resources and travel offices to complete the policy review and the initial technical transition. The USDS’ Defense Digital Service team assisted DoD and its DTS contractor in identifying a commercial vendor that could meet its requirements without requiring expensive customization.

The Defense Digital Service team is also helping DoD pilot this new system. The pilot, now underway, is focused initially on a small population of "basic travelers" using a streamlined travel policy subset. Over time, the project will scale in size and complexity. Concurrently, an effort is underway to considerably simplify the JTR by consolidating the types of travelers.

Success Criteria	Status
New DTS tool released	In progress. Tool has been identified, and is currently being piloted.
Policies governing DoD travel simplified	In progress. An effort is underway to considerably simplify the JTR by consolidating the types of travelers.
Increasing DTS customer satisfaction rating	In progress. As of June 2016, pilot is underway.

Success Criteria	Status
All travel request processed in new DTS system	Incomplete. Small pilot underway.
Improve data collection to enable better market position with travel vendors	Incomplete. Underway.

Milestones

- March 2015: DTS Sprint begins.
- June 2016: First user booked travel in the new system.

The Process and Lessons Learned

1. **Digital services are only as good as their underlying policy.** Many of the challenges with the current DTS system stem from the complexity of the Joint Travel Regulations. Without updates to this policy, it will be difficult to modernize the DTS. For example, the Joint Travel Regulations require pre-obligation, which is the act of obligating funds for travel prior to the trip based on the trip's estimated cost. This pre-obligation estimate is intended to prevent a trip from costing more money than is available, and includes transportation, hotel, per diem, and incidentals. However, many standard commercial travel solutions cannot easily accommodate pre-obligation estimates, so the DoD is working to change the current policy requirements to avoid requiring system customization. One solution being proposed is to estimate total travel costs and make a budgetary hold on the funds so that approving official will not approve trips in excess of an approved budget. Another potential solution also includes making an estimated bulk obligation based on historical expenditures.

2. **Test services with users as early as possible.** While the new system is being developed for use by all users, DoD is piloting it with certain types of travelers who have basic requests. DoD is following an industry best practice of launching systems earlier in their development, even when not all aspects may be fully automated. This will enable the team to improve the system based on real-world usage information.

3. **Use commercial cloud software services when possible, but be wary of commercial solutions that require extensive customization.** The modernized Defense travel system is being delivered using a commercial software-as-a-service travel tool, allowing DoD to avoid an unnecessary custom software development project. This is a best practice to follow when the commercial solutions require minimal customization to meet the government's needs. The DoD is seeking to avoid custom configuration requests for this service as much as possible, understanding that the expense and difficulty of such customizations often negate the benefits of using commercial services, and can lead to vendor lock-in.

4. **Modernization efforts should have clearly defined objectives.** If the success criteria above are met, this will enable the DOD to achieve the three main goals of modernizing the DTS: 1) Provide users a better customer experience, 2) increase the volume of trips, travelers and trip types processed with the system, and 3) save the Federal Government money. By clearly defining the strategic objectives of the effort, the delivery team can stay focused on what's important. In the absence of such a strategy, technical and policy constraints can drive product decisions.

Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon

The Challenge

The Department of Defense (DoD) spends billions of dollars every year on information security. However, the DoD had not yet taken advantage of a "bug bounty" approach to identifying security vulnerabilities that has gained traction in the private sector.

In this "bug bounty" approach, private citizens and organizations are invited to probe specific services for potential security vulnerabilities, and are rewarded for qualifying vulnerabilities they uncover and responsibly disclose to the sponsoring organization. In this way, private citizens are provided a legal way to disclose potential vulnerabilities without fear of retaliation or prosecution, and are given an incentive for doing so. Private sector companies have successfully used this approach to improve the security of their systems. Despite this technique's acceptance as an industry best practice, the government had not attempted such an initiative before.

Project Impact Summary

- In January 2016, the Digital Service team at DoD (Defense Digital Service) got approval for the Hack the Pentagon program, inviting private citizens to find and get rewarded for uncovering vulnerabilities in its information security system.
- This "bug bounty" approach mirrors that used by companies like Facebook and Twitter to catch more vulnerabilities and cost-effectively improve security.
- DoD contracted HackerOne – a well-known bug bounty platform startup with a strong reputation in the hacker community – to run the program.
- The digital services team, in conjunction with the existing vendors, worked in near real-time to fix security flaws as they were disclosed.
- The program led to the resolution of 138 previously unidentified vulnerabilities and cost $150,000. Contracting an outside firm to do a similar audit would have cost an estimated $1M and possibly still would not have provided the same security coverage.
- In June, the Secretary of Defense announced that DoD would run a persistent bug bounty program, and efforts are being made to share the practice with other agencies. There are also additional bug bounties the DoD will be running through the month of December.

The Solution

On April 18, 2016, the DoD, supported by the USDS' Defense Digital Service team, launched the first bug bounty in the history of the Federal Government. This innovative effort adopted from the private sector provided authorization to security researchers – "hackers" – to attempt to hack limited public-facing DoD systems and report vulnerabilities in exchange for financial rewards. This crowdsourced solution used the talent of over a thousand individuals, 250 of whom submitted at least one vulnerability report. Of these, 138 vulnerabilities were determined to be legitimate and unique. These had escaped notice from previous penetration tests DoD conducted. Using this information, DoD resolved all of the vulnerabilities.

While the program was underway, the Defense Digital Service team held daily calls with all agency stakeholders for everyone's situational awareness in regards to bounty activities. There was also a pre-determined escalation process in place to follow in case of an immediate, critical need for defensive action against out-of-scope activity.

For the first challenge, the DoD contracted with HackerOne, an experienced administrator of bug bounty programs that performs services for companies such as Yahoo, Square, and Twitter. This strategy worked well for several reasons: HackerOne already had a strong reputation and relationship with the hacker community, they could quickly sub-contract a private background check firm, they receive and triage vulnerability reports, and they are able to allocate payouts for qualifying bounties. Using a third party platform also served to quell any concerns of hackers about providing personal information to the DoD as part of a larger effort to create a hacker database.

The cost of the program was $150,000. DoD estimates hiring an outside firm to perform a comparable security audit and vulnerability assessment would have cost more than $1 million.

In early June, Secretary of Defense Ash Carter announced his plan to launch a persistent DoD Bug Bounty program to continue to allow hackers to be paid for discovering security flaws in specific DoD websites, applications, binary code, networks, and systems. To make this possible, he had the Defense Digital Service take on three initiatives: run more bug bounty programs for other DoD components in 2016; develop a Vulnerability Disclosure Policy that would firmly and clearly express that hackers are acting legally when they surface DoD vulnerabilities; and provide guidance for the future acquisition of services like those provided by HackerOne.

To date, two new bug bounty programs are in the planning stages. The disclosure policy has been drafted, circulated, and is on track for release by the end of 2016. Acquisition guidance is in progress. The contract with HackerOne has been renewed, and is a model for future contracts not just at DoD, but government-wide. Altogether, these efforts will help the Defense Digital Service work with interagency teams to advise on implementing similar bug bounty programs. There will also be a "Government Only" day for agency stakeholders to gather and gain insight on Hack the Pentagon's model of success.

Success Criteria

Success Criteria	Status
Engage the hacker community.	Complete. 1,400 Registered Participants

Success Criteria	Status
Identify and fix previously unknown security vulnerabilities.	Complete. 138 vulnerability reports were determined to be legitimate, unique and actionable for remediation. DoD fixed all vulnerabilities identified.
Resolve vulnerabilities at a cost lower than would be possible with other methods.	Complete. The total contract cost was $150,000, with approximately half of this paid as bounties to participants. With 138 actionable vulnerability reports, that equates to less than $1,100 per vulnerability. DoD estimates it would have cost $1M for an outside firm to perform a similar security audit.

Milestones

- January 2016: Hack the Pentagon program approved.
- March 2016: Contract signed to start the program.
- April 2016: Challenge start date and bounty start date.
- May 2016: Bounty end dates.

The Process and Lessons Learned

1. **Provide a method for outside individuals to responsibly disclose security vulnerabilities.** Many private citizens have an interest in uncovering security issues. Private sector companies often provide such individuals a legal, secure way to disclose vulnerabilities without fear of retaliation or prosecution. Hack the Pentagon has shown that the "bug bounty" approach can work well for the government. Even if there is no active bug bounty program, providing researchers a way to provide responsible disclosure of vulnerabilities could yield results.

2. **Ensure the agency is prepared to remediate vulnerabilities as they are discovered, in near real-time.** DoD took the important step of putting a team

on standby that could implement fixes to the vulnerabilities as they were disclosed. Being able to quickly address issues helped ensure no malicious activity could take place.

3. **Involve stakeholders early.** Running a new type of program in government can be complicated. The Defense Digital Service team worked closely with the DoD Office of General Counsel to resolve legal questions around bug bounty payments, participant background checks, and whether bounties could be paid to U.S. Government personnel.

Section 3

Other USDS Initiatives

Hiring Top Technical Talent

The Challenge

In order to deliver on the mission of transforming the country's most important digital services, the Federal Government needs an infusion of modern software engineering, design, and product management skills. As demonstrated in earlier sections of this report, pairing individuals with these skills with dedicated civil servants across the Federal Government can dramatically accelerate modernization efforts on major IT acquisition projects.

However, hiring individuals with these skills has been challenging for the Federal Government for several reasons:

- It is difficult to attract highly qualified applicants to apply for government technology positions.
- The Federal Government often provides a candidate experience that is not competitive with the private sector in terms of timeline, ease of application, and frequent communication of application status.
- It is challenging to properly evaluate these highly specialized and technical skills in order to select the most qualified individuals from among all applicants.

One of the early priorities of the USDS was to build a robust recruitment and hiring program that could address these challenges.

Project Impact Summary

- It is difficult to attract highly qualified applicants from the private sector to apply for government technology positions, as the technology industry is one of the most competitive in the world.
- USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent.
- Mirroring technology industry best practices, USDS built an experienced recruiting team who sources software engineering, product management, and design professionals from industry.
- USDS provides candidates with an easy application process and a fast timeline for hiring decisions, averaging 34 business days from application to conditional offer.

- USDS hiring process has a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists, including those who did not receive offers.
- USDS uses subject matter experts to evaluate specialized skills.
- USDS has shortened the personnel security process from 67 days to 20 days.
- USDS reached its goal of recruiting 200 digital service experts by the end of 2016, ahead of schedule.

The Solution

USDS partnered with OPM to secure the tools necessary to recruit and hire the country's brightest technical talent. Using these tools, we created a recruiting and hiring operation that draws on several private sector best practices.

- **Engage in Targeted Recruiting Activities**. Mirroring private sector best practices, USDS has built an experienced recruiting team tasked with identifying and encouraging a diverse set of qualified applicants to apply for digital service positions. Specific tactics include targeted outreach to technology and design professionals (including those who are not currently seeking a new job), events, roundtables, and building a network of influencers who can validate the importance and professional respectability of the USDS' public service mission.

- **Focus on Candidate Experience**. The USDS hiring process puts a premium on providing a high quality candidate experience that is competitive with the private sector. Specifically, the USDS aims to provide candidates with an easy application process (currently delivered via the website), a fast timeline for hiring decisions (targeting 15 business days from application to conditional offer for qualified applicants), and good visibility into the process and application status.

  USDS measures its effectiveness by asking all candidates who complete the hiring process to complete a satisfaction survey, and target a satisfaction score of 4.5 or greater (out of 5.0) from among all finalists (including both those who receive offers and those who do not).

- **Use Subject Matter Experts to Evaluate Specialized Skills.** Evaluating applicants with highly specialized skills is a challenging practice that requires subject matter expert involvement at every stage. USDS has fully embraced the use of such experts in the hiring process. Each candidate for the USDS is evaluated by a panel of engineers, designers and product managers who themselves possess the desired specialized skills. By ensuring that applicants are evaluated by technical specialists within their own discipline, the process ensures

that individuals selected for USDS roles have the digital expert skills that are required to improve government technical services.

This hiring program is run centrally from the USDS headquarters unit inside OMB, so that all chartered USDS teams can benefit from a dedicated recruiting operation and a standardized, rigorous selection process.

Success Criteria	Status
Hire 200 Digital Service Experts by end of 2017	On track to meet target ahead of schedule. 196 Digital Service Experts hired as of September 2016.
Days from Application to Conditional Offer = 15 business days	In progress. Time reduced from 55 days in Q4 2015 to 34 days in Q3 2016.
Day from Conditional Offer to Final Offer (personnel security process) = 16 days	In progress. Time reduced from 67 days in Q4 2015 to 20 days in Q3 2016.
Candidate Satisfaction Score for going through the hiring process is 4.5 (or above) out of a scale from 1 to 5 (5 being the most satisfied)	On track. Average candidate satisfaction since Q4 2015 is greater than 4.5.

Transforming Federal IT Procurement

The Challenge

Government procurement cycles do not keep pace with fast-changing technology and user needs. This is largely due to a reliance on waterfall development methods where requirements are defined and documented in full detail before any design, development or user testing can take place. When tied to inflexible contracts, this approach makes it very difficult to build an easy to use, effective digital service. Adapting patterns and best practices from private industry will allow the Federal Government to deliver products faster, cheaper, and at higher quality.

Project Impact Summary

- The USDS procurement team has launched several projects to help the Federal Government enter into better, more agile contracts and buying decisions.
- The objective is not only to change the way IT services and products are acquired, but to model new procurement processes for the government at large.
- During a discovery sprint, the USDS team made recommendations for modernizing SAM.gov, the system businesses use to receive contracts and grants from the Federal Government.
- The GSA has accepted the recommendation to move SAM.gov to a Common Services Platform, allowing developers to make speedier improvements to the existing system, automate more services, and increase security.
- USDS also advised SBA to consolidate certification systems for small businesses seeking government contracts. SBA has since moved to a modern technology stack, and will soon process all certifications through certify.sba.gov.
- In October 2015, USDS and OFPP launched the Digital IT Acquisition Professional Training (DITAP) program, piloting a course that successfully taught federal contracting professionals material relevant to digital services procurement.
- USDS and OFPP are now working to transition this program to GSA and other Federal Government agencies.
- Also in partnership with OFPP, USDS developed the TechFAR Handbook, and the TechFAR Hub, to advise all federal agencies on how to adopt more flexible acquisition practices.

The Solution

USDS has a dedicated acquisition team working to improve the government technology marketplace and to help the government make better buying decisions. The USDS procurement team has launched several solutions since its inception and continues to evaluate new potential solutions.

System for Award Management (SAM.gov)

In order for businesses to receive a contract or grant from the government, they are required to register in the General Services Administration's (GSA) System for Award Management (SAM.gov). However, because the process is so cumbersome, many businesses are discouraged from engaging with the government. The USDS and GSA completed a two-week discovery sprint in March 2016 to define what a successful SAM.gov modernization would look like. This included evaluating the technology, business processes, and the customer experience underlying SAM and the related Integrated Award Environment.

USDS' recommendations from the discovery sprint included:

- **Shift from Process to Product.** In order to develop and ship such a large solution, the work must be centered around the idea that it is delivering a federal-wide product capable of meeting the demands and objectives of various and competing end user needs.
- **Invest in the Team.** Rather than hiring external experts, or bringing on other teams, GSA should make an investment in and prioritize comprehensive and frequent training for all roles within its Integrated Award Environment, from management to external stakeholders to contracting officers.
- **Empower a New Team Culture.** The unified team has the potential to deliver a powerful digital service by adopting a culture that embraces change, challenges the status quo, and does not accept anything less than excellence. The ideal team is self-motivated to look at everything as an opportunity to solve end users' problems.
- **Deliver. Deliver. Deliver.** The main benefit for adopting an agile development methodology is the ability to accelerate product delivery. Leadership must dissolve any fears of failure that create hesitancy when making a change to a product—whether it's prototypes, beta versions, or enhancements. The team has universally expressed a willingness to move to continuous integration, rapid delivery model, and USDS provided a 6-month plan for this transition.

- **Migrate to a Secure, Robust Services Platform.** The SAM.gov environment is transitioning to a Common Service Platform that will allow applications to be built on top of an infrastructure layer. Adopting continuous integration, implementing the "DevOps" practice of integrating system operations with application development teams and processes, and establishing protocols for a multi-vendor environment to implement changes on the new platform would speed improvements. In addition, there should be a drive to automate services and provide real-time data, such as TIN validation. To improve security, USDS recommended SAM.gov implement host segmentation and network security controls for restricting access to sensitive data on the Secure FTP service. Other key areas of opportunity recommended to improve the basic platform include open-source, standardization, and implementing a mitigation strategy for DDoS protection aligned with the public release of services on the Common Service Platform (CSP).

GSA has accepted the recommendations and is in the process of making nearly all of the changes. They have already restructured their team based on functions and are working cohesively in a team based environment.

Small Business Certifications

It is part of the mission of the Small Business Administration to expedite small businesses' access to government contracts. Better utilization of the 8(a) Business Development, Women-Owned Small Business (WOSB), HUBZone, and Service Disabled Veteran Owned Small Business Programs would serve this mission.

In early 2015, SBA asked the USDS to help it modernize and consolidate the systems that power these certification programs. After USDS personnel conducted an initial technical evaluation, the USDS procurement team assisted SBA in developing a contract to create a modern system using the best practices described in the Digital Services Playbook. SBA has since awarded an agile software development contract for revamping these certification processes as part of the SBAOne project.

In just 5 months following the award of the contract, SBA moved to a modern technology stack, hosted on flexible public cloud infrastructure, and launched an eligibility service in December 2015 for the WOSB program. This release was shortly followed by the successful launch of the modernized Woman-Owned Small Business certification system in March 2016 on certify.SBA.gov. Work is underway for the modernization of the 8(a) certification program, for a release planned in early 2017. Eventually all SBA Certifications will be processed through Certify.SBA.Gov.

Digital IT Acquisition Professional Training (DITAP)

Helping the government become smarter buyers requires the establishment of a specialized and educated procurement workforce that understands the digital and IT marketplace, utilizes best practices for IT purchasing, and capitalizes on the power of the government acting as a single purchasing entity and the economies of scale this provides. To achieve this, the USDS and the Office of Federal Procurement Policy (OFPP) have partnered to develop a digital IT acquisition professional community (DITAP).

The first component of this community was a training and certification program for contracting officers. USDS and OFPP posted a prize competition on Challenge.gov in May 2015 to develop the Digital Service Contracting Professional Training and Development Program for the Federal Government. As a part of this process, USDS and OFPP held a Reverse Industry Day where 70 representatives from vendors familiar with agile software development techniques, system integrators, collegiate entities, and training developer came together to confirm that the specific training did not yet exist and confirm that the Challenge.gov platform would be an effective path forward in developing the training. In all, 23 submissions were received, 3 finalists provided mock classroom presentations of their content and assessment plan, and by October 2015, the final winner began its finalized 6-month course with the first class of 30 Contracting Professionals from 20 federal agencies.

Over the 6 months, the attendees completed 11 days of classroom training on agile software development methodology, cloud hosting, and the "DevOps" practice of integrating system operations with application development teams and processes. The attendees completed 120 hours of self-directed learning and webinars, heard from 10 guest speakers, supported 6 live digital assignments, and completed a final capstone assessment of skills. Since the course ended in March 2016, 6 participants received promotions or changed job roles to take on IT work, 12 participants were assigned digital service acquisition work or are working with an agency digital service team, and two were named agency Acquisition Innovation Advocates. 90% of the 28 graduates felt they were ready to conduct digital service acquisitions in their agency. USDS and OFPP are restructuring the next round of implementation based on these results. The second class began in July 2016.

USDS and OFPP are currently training Federal Acquisition Institute (FAI) facilitators on how to conduct the program, for transfer of responsibilities in FY17. In addition, USDS and OFPP are finalizing the Federal Acquisition Certification in Contracting (FAC-C) Digital Service certificate program requirements and encouraging the development of similar training programs for government Contracting Officer Representatives and Project Managers. The long-term goal is for any federal training institution to be able to

use and update the course material in an open source manner to create their own development program without incurring the cost of content.

Success Criteria	Status
60 Contracting Officers trained in digital service acquisition.	In progress. 28 completed pilot. 30 started next round in July 2016

TechFAR Handbook

In the Government, digital services projects too often fail to meet user expectations or contain unused or unusable features. Several factors contribute to these outcomes, including, overly narrow interpretations of what is allowed by acquisition regulations. The Office of Federal Procurement Policy, with the assistance of the USDS, developed the TechFAR to highlight flexibilities in the Federal Acquisition Regulation (FAR) that can help agencies implement "plays" in the Digital Services Playbook.

The TechFAR is a handbook that describes relevant FAR authorities and includes practice tips, sample language, and a compilation of FAR provisions that are relevant to adopting an agile style of software development as the primary means of delivering software solutions. Agile software development is a proven commercial methodology characterized by incremental and iterative processes where releases are produced in close collaboration with the customer. The TechFAR facilitates a common understanding among agency stakeholders of the best ways to use acquisition authorities to maximize the likelihood for success in agile contracts and there is nothing prohibitive in the Federal Acquisition Regulations for adopting these methods and re-engineering contracts to support delivery of quality products. This handbook is a living document; users are urged to provide feedback, share experiences, and offer additional strategies, practice tips, policies, or contract language that may be used to assure that IT acquisitions achieve their desired results.

USDS also released the TechFAR Hub on GSA's Acquisition Gateway. The TechFAR Hub is designed to advise all federal agencies on how to implement best practices, as described in the digital service playbook and TechFAR, and as a community space for digital service practitioners.

Supporting the Development of Federal Shared Services

Shared technology platforms and services have the potential to simplify government products, increase consistency, reduce development costs, and eliminate duplication. Security also benefits by focusing resources on a smaller number of key components.

USDS is uniquely positioned to support the development of these shared services, because it works across many agencies and has visibility into many of the government's digital service development efforts. This insight enables USDS to invest in developing and promoting reusable platforms and services.

Project Impact Summary

- USDS supports the development of shared technology platforms and services because they have the potential to simplify government products, increase consistency, and reduce development costs.
- In May 2016, a USDS and 18F team began implementation work on Login.gov, a service that will provide a secure and user-friendly login process for multiple government digital services. Login.gov is currently being integrated with its first agency customer.
- Many government digital services are siloed under unique brands and programs, leading agencies to spend time and money redesigning common digital components such as buttons, forms and search bars. In September 2015, USDS and 18F released the U.S. Web Design Standards, a set of components that agencies can adopt to provide their users a consistent, high quality online experience while reducing the chance of duplicative work. Moving forward, GSA will continue to develop the Standards. Since its release, the standards have been downloaded over 17,000 times.

Login.gov Consumer Identity Platform

Many consumer-facing government digital services require individuals to create user accounts in order to access the service. The USDS has helped several agencies implement such systems, including at USCIS, CMS, SBA and IRS. Many more agencies have already implemented their own solutions. Despite several earlier attempts to build a common identity management platform, no such platform has been widely adopted.

Providing a secure and user-friendly login process for the government's digital services would improve the experience of interacting with government services, and help agencies implement digital services faster and more securely. To that end, the USDS and the General Service Administration's 18F are working iteratively with a team of technologists from across the Federal Government to build a platform for users who need to log in to government services. The team is coordinating with the Federal Acquisition Service, the Office of Management and Budget, and the National Institute of Standards and Technology on the specifics of the platform.

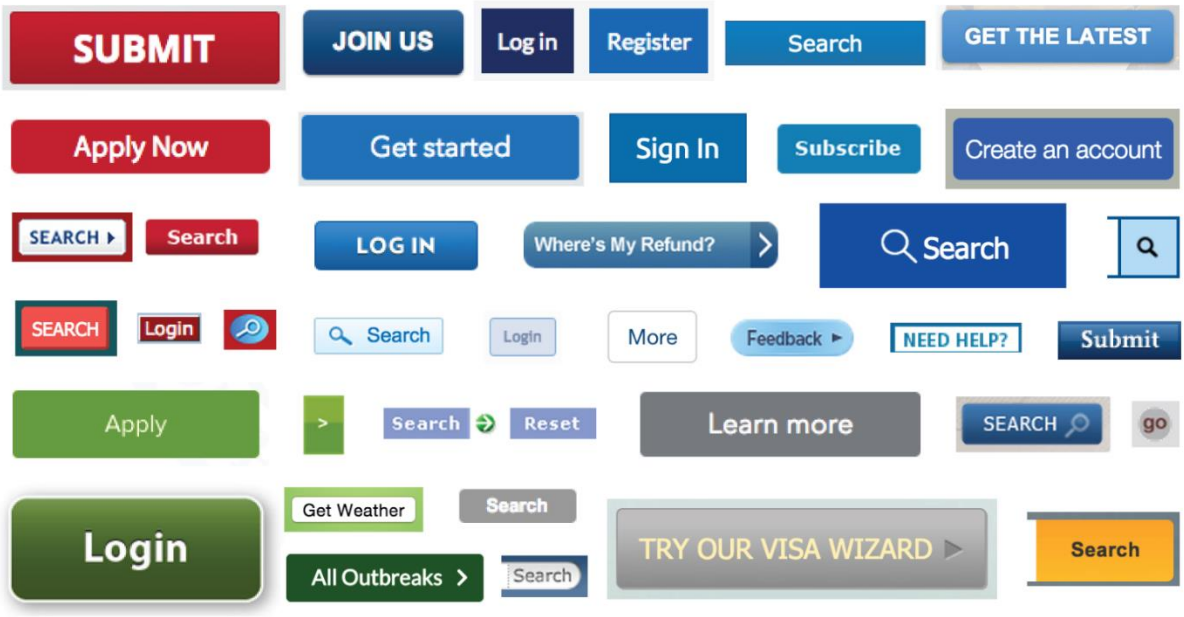
To build the Login.gov platform, the team is using modern, user-friendly, strong authentication and effective identity proofing technology. The project builds off of the hard work that was already done to create and implement the Connect.gov pilot, an earlier project with similar goals. The team is also using lessons learned from our counterparts in the UK who built GOV.UK Verify. More specifically, the team will accomplish these goals by:

- Creating a simple, elegant way for the public to verify their identity, log in to federal government websites, and, if necessary, recover their account
- Building experiences, processes, and infrastructure that will use the latest available technology to safeguard all user data
- Delivering software that will allow government developers to integrate it within hours, not weeks
- Iteratively improving the system throughout its lifetime
- Preserving privacy including mitigating risks and adhering to federal privacy guidelines
- Following security best practices including implementing easy-to-use multi-factor authentication

The team has identified the first agency to adopt this shared platform, and is in talks with several additional agency customers to be the second adopter early in 2017. Based on the success of the first two initial adopters, the team will scale out the adoption in 2017.

U.S. Web Design Standards

When members of the public access government services online, they're often met with confusing navigation systems, conflicting visual brands, and inconsistent interaction patterns — all factors that can erode trust in our government's services.



A snapshot of buttons across government websites

Recognizing the necessity of consistent, easy-to-use design, many agencies have started creating their own design patterns and user interface (UI) toolkits, but their efforts are often duplicative. Because many digital services are siloed under unique brands and programs, the Federal Government runs the risk of spending time and money reinventing the wheel — that is, recreating common patterns such as buttons, forms, and search bars that already exist. What's more, creating pattern libraries and toolkits is a time- and labor-intensive process, and one not all agencies have the resources to support.

Designers and developers at USDS and 18F teamed up to address the need for consistent, accessible design components. Together, they created the Draft U.S. Web Design Standards (the "Standards"), a set of open source UI components and a visual style guide that agencies can use to create consistent online experiences. The Standards, which launched in September 2015, follow industry-standard accessibility guidelines and draw on the best practices of existing style libraries and modern web design. To offer the highest-quality product, the Standards team makes frequent updates to introduce new features, fix bugs, provide clearer documentation, and more.

Agencies using the Standards enjoy several distinct benefits. Not only are they providing an enjoyable, consistent user experience, but they're also saving design and development time that can be dedicated to other projects. Using the Standards, a team can build a site quickly and with minimal effort, allowing their agency to communicate its message more effectively.

Moving forward, GSA's 18F team will continue to develop the Standards.

Success Criteria	Status
Overall Goal: Begin implementation of at least one outstanding common platform by end of 2016.	Complete. Implementation of shared login platform began in May 2016. Draft U.S. Web Design Standards released September 2015.
Sub-Goal: Draft U.S. Web Design Standards available for agency use.	Complete. Initially released in September 2015, they include an online style guide and downloadable software package. The standards have been downloaded more than 17,000 times. As of September 2016, more than 78 people have contributed to the Standards' code base, and more than 200 people have participated in conversations on the Standards' GitHub repository. The Standards team welcomes outside recommendations and contributions, which help drive the project's process forward.
Sub-Goal: At least three agencies have adopted a shared login service.	Incomplete. Development of an interagency login system is in progress, but it is not in use yet. Initial agency customer identified.

Milestones

Web Design Standards

- September 2015: Draft U.S. Web Design Standards released

Consumer Identity Platform

- December 2015: Identity sprint completed

- January 2016: Research starts
- May 2016: Implementation begins

Exhibit 37

U.S. tells Arkansas to delete files on voter data

By Bill Bowden , Brian Fanney twitter
This article was published today at 4:30 a.m.

Arkansas voter data provided to President Donald Trump's voter-fraud commission is headed for the trash days after it was submitted.

According to an email exchange obtained Wednesday under the state Freedom of Information Act, Andrew Kossack, associate counsel for Vice President Mike Pence, asked officials in Secretary of State Mark Martin's office to delete from a federal server the voter data it submitted.

However, state officials could not access the server.

"We were unable to access the SAFE site again in order to pull down the file, pursuant to your request," wrote Peyton Murphy, assistant director of the state elections division, in a Monday email. "We understand that the file has not yet been accessed, but that it will expire 14 days from the time of the upload."

Kossack replied that the federal site would delete the file.

"I'll be back in touch with next steps," he continued. "Again, thank you for your submission, and my apologies for this inconvenience."

Arkansas submitted its data on July 5. It was the first state to submit data to the Presidential Advisory Commission on Election Integrity.

The SAFE site -- also known as the Safe Access File Exchange -- is at the heart of a lawsuit filed by the Washington, D.C.-based Electronic Privacy Information Center. The file exchange is run within the Department of Defense.

Kossack referred to the lawsuit in his email.

[EMAIL UPDATES: Get free breaking news alerts, daily newsletters with top headlines delivered to your inbox]

The Electronic Privacy Information Center contends that the commission failed to conduct a privacy information assessment -- required under the E-Government Act of 2002 -- before collecting the data using the Department of Defense system.

"The 'SAFE' URL, recommend by the Commission for the submission of voter data, leads election officials to a non-secure site," according to the Electronic Privacy Information Center.

"Regarding this website, Google Chrome states: 'Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards).'"

In the initial request for information, dated June 28, Kris Kobach, vice chairman of the Presidential Advisory Commission on Election Integrity, noted that the commission wanted Arkansas data -- "if publicly available under the laws of your state" -- including names, addresses, dates of birth, political party affiliations, the last four digits of Social Security numbers "if available," voter history, voter status, felony convictions, information regarding voter registration in another state, military status and overseas citizen information.

The information submitted to the file exchange from Arkansas did not contain Social Security numbers, felony convictions, military status and driver's license numbers. Such information is not publicly available in Arkansas.

However, names, addresses, dates of birth, political party affiliations, voter history since 2008, registration status, email addresses and phone numbers -- were shared. The database does not say for whom someone voted -- only whether they voted.

The same Arkansas voter information that was released to the Trump administration has been provided about 200 times since January 2015 to various entities, Kelly Boyd, chief deputy secretary of state, told legislators and county clerks meeting Wednesday in Eureka Springs.

Those entities include states, organizations, political parties and Arkansas legislators, he told a crowd of about 100 at the Basin Park Hotel.

"We submit information every year to the state cross-check program, and we do that at no charge," Boyd said. "And we did that at no charge for this program."

"To be very clear on this, there was no sensitive information released, no Social Security numbers, no partials, no military data, no felon data, no data that you can't get out of the phone book."

Boyd said the data would reveal some voting information.

"They're going to know whether you voted R or D or O [optional] or N for nonjudicial in the primaries," said Boyd. "It would tell whether you voted E early, A absentee or P at the polls, back to 2008. ...

"I know there's been a lot of angst about that, and I'm sorry. I wish there hadn't been. This information is openly available. There are ways to make it not openly available. I'll work with you if you want to do that."

Gov. Asa Hutchinson told a group of high school students Monday that the state should not have provided any data to the Trump commission.

"I am not a fan of providing any data to the commission in Washington," Hutchinson said in response to a student's question.

"Even though it is publicly available information and anyone can get it -- all you have to do is file a Freedom of Information [Act] request to get the information -- I just don't want to facilitate the providing of that information to a federal database. I don't think that's helpful for us."

The governor spoke as Kossack and Arkansas secretary of state staff members were trading emails about deleting the Arkansas information.

Information for this article was contributed by The Associated Press.

Metro on 07/13/2017

Print Headline: U.S. tells state to delete files on voter data; But authorities in Arkansas unable to access federal site

Exhibit 38

DECLARATION OF MARC ROTENBERG

I, Marc Rotenberg, declare as follows:

1. I am President and Executive Director for the Plaintiff Electronic Privacy Information Center ("EPIC").

2. Plaintiff EPIC is a non-profit corporation located in Washington, D.C. EPIC is a public interest research center, which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), EPIC pursues a wide range of activities designed to protect privacy and educate the public, including policy research, public speaking, conferences, media appearances, publications, litigation, and comments for administrative and legislative bodies regarding the protection of privacy.

3. I am a member in good standing of the Bar of the District of Columbia (admitted 1990), the Bar of Massachusetts (1987), the U.S. Supreme Court (1991), the U.S. Court of Appeals—1st Circuit (2005), the U.S. Court of Appeals—2nd Circuit (2010), the U.S. Court of Appeals—3rd Circuit (1991) the U.S. Court of Appeals—4th Circuit (1992), the U.S. Court of Appeals—5th Circuit (2005), the U.S. Court of Appeals—7th Circuit (2011), the U.S. Court of Appeals—9th Circuit (2011), and the U.S. Court of Appeals—D.C. Circuit (1991).

4. I have taught Information Privacy Law continuously at Georgetown University Law Center since 1990.

5. I am co-author with Anita Allen of a leading casebook on privacy law.

6. In my capacity as President and Executive Director, I have supervised both EPIC's response to the Department's rulemaking and EPIC'S participation in all stages of litigation in the above-captioned matter.

7. The statements contained in this declaration are based on my own personal knowledge.

8. EPIC works with an Advisory Board consisting of nearly 100 experts from across the United States drawn from the information law, computer science, civil liberties and privacy communities.

9. Members of the EPIC Advisory Board must formally commit to joining the organization and to supporting the mission of the organization.

10. Members of the EPIC Advisory Board make financial contributions to support the work of the organization.

11. Members of the EPIC Advisory Board routinely assist with EPIC's substantive work. For example, members provide advice on EPIC's projects, speak at EPIC conferences, and sign on to EPIC amicus briefs.

12. In this matter, EPIC represented the interests of more than 30 members of the EPIC Advisory Board, who signed a Statement to the National Association of State Secretaries in Opposition to the Commission's demand for personal voter data.

Under penalty of perjury, I declare that the foregoing is true and correct to the best of my knowledge and belief.

Marc Rotenberg
EPIC President and Executive Director

Executed this 7th day of July, 2017

Exhibit 39

Trump election group backs away from its request for voter data after outcry

Commission on election integrity's 'repugnant' request for voter data prompted privacy concerns and numerous legal challenges

277

Andrew Gumbel in Los Angeles

Thursday 13 July 2017 05.00 EDT

The Trump administration is backing away from its extraordinary attempt to gather voters' personal information, following a barrage of legal challenges, an outcry from state officials, and a rash of voter registration cancellations by people concerned about their privacy.

Voting rights groups have filed at least six lawsuits in response to a letter sent out on 28 June by Kris Kobach, vice-chair of the presidential advisory commission on election integrity, asking state officials to provide names of the country's 150 million voters. In addition, the letter sought voters' addresses, social security numbers, voting histories, party affiliation, criminal histories, military status, and more.

Kobach has said the request is designed to help prevent fraudulent in-person voting. But his detractors say he is looking for a solution to a non-existent problem and suspect his true interest is in finding reasons to deny legitimate voters their rights, for partisan advantage.

Both Kobach and Trump have floated the notion that 3 to 5 million people voted illegally last November – a notion that has angered both Republican and Democratic election officials because there is no shred of evidence to support it.

> Trump's voter fraud commission is a shameless white power grab
> Steven W Thrasher
>
> Read more

Kobach's letter told states to comply with his request by 15 July, but the White House has already postponed that deadline pending a ruling from the Washington DC circuit court on one of the lawsuits. That ruling is not due until next week at the earliest.

The commission has also abandoned plans to store the information on a temporary Pentagon computer and promised to have a dedicated White House server ready to receive the data by next week.

Not one state – not even Kansas, where Kobach is secretary of state and in charge of elections – has agreed to comply fully with the request. Many have cited privacy concerns and other legal restraints. Only three states, Colorado, Missouri and Tennessee, have indicated any enthusiasm about complying. Many more have responded with fury, including Mississippi, whose Republican secretary of state memorably told Kobach to "go jump in the Gulf of Mexico".

Maryland's attorney general, Brian Frosh, called the request "repugnant". "It appears designed only to intimidate voters," he wrote, "and to indulge President Trump's fantasy that he won the popular vote."

According to the lawsuits filed by the Electronic Privacy Information Center (Epic), the American Civil Liberties Union (ACLU) and others, Kobach's request sidestepped clear legal requirements on privacy protection – the issue that prompted the White House to hold off on its deadline.

The suits also accuse the commission of working at a constitutionally intolerable level of secrecy, and Kobach himself of blurring the legal lines between his position as vice-chair and his candidacy in next year's Kansas gubernatorial election.

Epic's complaint and call for a temporary restraining order, filed this month, denounced the proposed voter database as "unnecessary and excessive" and said the commission risked violating "the informational privacy rights of millions of Americans" and exposed the country's electoral system to potential new forms of registration and voter fraud. To make the information gathered by the commission public, it added, would be "both without precedent and crazy".

Donald and Melania Trump cast their votes in the 8 November 2016 presidential election. Photograph: Evan Vucci/AP

Two of the suits, by the ACLU and the Lawyers' Committee of Civil Rights Under Law, seek to postpone the presidential committee's next meeting, set for next Thursday, unless the White House discloses its communications about the meeting and opens it to the public.

Voting rights activists are hoping that the legal and political pressure will induce the White House to drop the data-gathering exercise altogether. "The program was ill conceived and poorly executed," Epic's president and executive director Marc Rotenberg said in a statement. "We expect the commission will simply announce that it has no intention, going forward, to ask the states for their voter records."

Some damage, however, has already been done, as election officials in at least four states – Arizona, Colorado, Florida and North Carolina – report receiving requests from hundreds of voters to cancel their registrations to protect their personal information.

Local voting officials were bombarded with email requests and phone calls after the Kobach letter became public. In some cases, the officials talked voters out of cancelling their registrations, arguing that the data was in the system already and they would only be damaging themselves. In other cases, voters said straight out they did not trust the presidential commission. One North Carolina voter said it "smells funny".

The voter response in Arizona appears to have triggered a change in policy. The secretary of state there initially said she would be withholding social security numbers, dates of birth and other identifying details but otherwise complying with the request. By the time she sent her official response, however, the line had changed to a flat no.

Exhibit 40

Arkansas Voter Registration Data

The Arkansas Secretary of State's Office provides three different statewide voter registration data files.

The first is the statewide Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted.

The second file contains the Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle. The older elections are incomplete since some counties did not enter voter results into the previously used VR databases. The Vote History file does not contain voters' names and therefore must be linked to the Voter Registration file by a unique Voter ID # found within each file.

The third file is a combination of the Voter Registration and Vote History files (VRVH).

- All files are ASCII text files with comma delimited, double quoted fields. This is commonly called comma-separated values format or .CSV format.
- Since there are about 1.6 million records in each, the files will not fit into an Excel spreadsheet.
- The VR file size is about 585 MB, the Vote History file size is about 402 MB, and the Combo file is about 1 GIG. Due to the file size no files can be sent via email.
- The cost per file is $2.50.
- The file(s) are available in CD format for pickup at the State Capitol Building or by mail. These files can also be placed on an FTP site if desired.

We are often asked the question, "Are there any restrictions on the use of this data?"
Currently there are no state laws that place restrictions on the use of data that we release. However, there are Federal and State laws that restrict some fields on the VR record from being released (Arkansas Code, Amendment 51§ 8(e)). These fields are never released and are never on any file that our office provides to the public.

To request a file you may complete the Data Request Form on the following page.

Data Request Form

Date: _____ Request taken by: _____

Contact Name: _____ Telephone: _____

Email Address: _____

Please check one of the following: Do you wish to…

Pick up the data ____ ***Have the data placed on your FTP site____***
Have the data mailed to the address below ____

Company: _____

Address: _____

City, State, Zip: _____

Data Requested, Comments and Instructions: _____

_____

_____

_____

_____

Number of Data Disk(s)/File(s)/Report(s) created: _____ created by: _____
Data Disk(s) filename(s): _____

_____

Please remit $2.50 for each enclosed Data Disk(s)/File(s)/Report(s)

Number of Data Disk(s)/File(s)/Report(s) created: _____ Total Cost:_____

Make Check or Money Order payable to: **Arkansas Secretary of State**

Mail payment to: ATTN: Data Request
Arkansas Secretary of State
State Capitol Bldg, Room 026
Little Rock, AR 72201

Any questions regarding this data should be reported to the Office of the Secretary of State at 1-800-247-3312 or via email at voterservices@sos.arkansas.gov .