ALASKA STATE LEGISLATURE
JOINT MEETING
SENATE STATE AFFAIRS STANDING COMMITTEE
SENATE JUDICIARY STANDING COMMITTEE
October 28, 2021
9:02 a.m.

MEMBERS PRESENT

SENATE STATE AFFAIRS

Senator Mike Shower, Chair (via teleconference)
Senator Lora Reinbold, Vice Chair (via teleconference)
Senator Mia Costello
Senator Roger Holland
Senator Scott Kawasaki (via teleconference)

SENATE JUDICIARY

Senator Roger Holland, Chair
Senator Mike Shower, Vice Chair (via teleconference)
Senator Shelley Hughes (via teleconference)
Senator Jesse Kiehl (via teleconference)

MEMBERS ABSENT

SENATE STATE AFFAIRS

All members present

SENATE JUDICIARY

Senator Robert Myers

OTHER LEGISLATORS PRESENT

Representative Kevin McCabe (via teleconference)

COMMITTEE CALENDAR

PRESENTATION(S): CYBERSECURITY ISSUES and SOLUTIONS

- HEARD

PREVIOUS COMMITTEE ACTION

No previous action to record

WITNESS REGISTER

BURKE STEPHENSON, Freelance Cybersecurity Consultant
Cybersec Innovation Partners
London, England
United Kingdom
POSITION STATEMENT: Delivered a presentation on cybersecurity issues and solutions.

MEGAN WALLACE, Director
Legislative Legal Services
Legislative Affairs Agency
Alaska State Legislature
Juneau, Alaska
POSITION STATEMENT: Provided legal advice about meeting in executive session during the presentation on cybersecurity issues and solutions.

ACTION NARRATIVE

9:02:10 AM
CHAIR ROGER HOLLAND called the joint meeting of the Senate State Affairs Standing Committee and the Senate Judiciary Standing Committee to order at 9:02 a.m. Present at the call to order from the Senate State Affairs Committee were Senators Costello, Holland, and Chair Shower (via teleconference). Present from the Senate Judiciary Committee were Senators Kiehl (via teleconference, Hughes (via teleconference) and Chair Holland. Senate State Affairs Committee member, Senator Kawasaki and Senate Judiciary Committee member, Senator Reinbold joined the meeting thereafter (via teleconference).

PRESENTATION(S): Cybersecurity Issues and Solutions

9:03:27 AM
CHAIR HOLLAND stated that the legislature is in the 4th Special Session of the year and while cybersecurity is not included in the call, an opportunity arose to hear from freelance cybersecurity consultant Burke Stephenson who works for Cybersec Innovation Partners. He will present information regarding cybersecurity issues and solutions, particularly as they apply in Alaska. He asked Senator Shower if he had any opening comments.

9:04:17 AM
CHAIR SHOWER apologized for not being able to attend the meeting in person and thanked Chair Holland for stepping in at the last moment to chair the meeting in his stead.

9:04:50 AM
At ease

9:06:03 AM
CHAIR HOLLAND reconvened the meeting.

9:06:55 AM
BURKE STEPHENSON, Freelance Cybersecurity Consultant, Cybersec Innovation Partners (CIP), stated his intention to educate legislators about cybersecurity and why it is important not just to the State of Alaska, but industry wide.

He began the presentation with a quote from John F. Kennedy who said, "There are risks and costs to action. But they are far less than the long-range risks of comfortable inaction."

9:08:07 AM
MR. STEPHENSON said he would set the stage by repeating the statement he made to Senator Shower last month. He paraphrased his remarks, which read:

[Original punctuation provided.]

> The State of Alaska has suffered 4 separate cyberattacks in less than 2 years. We have been informing and providing evidence directly to Alaska over the last 18 months of why. This is because Alaska's current IT and cyber vendors are NOT providing adequate protection, and Alaska's IT infrastructure in Insecure. This is an obvious statement, unfortunately what we see every day is that the obvious is constantly being overlooked.
>
> Over the next few minutes, I am going to define and explain, with irrefutable evidence why this statement is indicative of the cyber security posture for all industries, businesses, business verticals, and is systemically causing billions in losses and costs, nothing will change unless we change it. This also includes the Alaskan Government.

9:09:12 AM

MR. STEPHENSON deviated from his prepared statement to report that cybercrime is the third largest economy in the world, after those of the U.S. and China. He reported that in 2021 cybercrime will produce $6 trillion. It is even more profitable than the global drug trade, which is more than all national disasters combined.

9:09:51 AM
MR. STEPHENSON paraphrased the last paragraph on page 1 of the presentation, which read:

[Original punctuation provided.]

> In this special session on voting integrity this report is one of the most important parts of ensuring voter integrity. If a voter registration of Alaska Department of Elections website can be breached, which have been and still can be, then all data and information, including the integrity of the voter's identification, is all at risk of manipulation.

MR. STEPHENSON stated that all state agencies are vulnerable because the government is interconnected. He advised that he provided examples to show that cybercriminals eventually will gain entry if there is an access point. Once they have gained access, these cybercriminals are able to access information, including voter information and possibly manipulate or steal the data.

9:11:09 AM
MR. STEPHENSON paraphrased the introduction on page 2 of his remarks, which read:

[Original punctuation provided.]

> Before I start, I want to again thank you for this opportunity. I am honored and humbled to be asked to present to you in one of our Nation's greatest establishments in the assurance of justice and freedom. I am honored, that in my realm of experience and professional expertise I have been asked to provide this statement to you regarding the cyber security posture of Alaska's State Government. I am humbled, humbled because of the constant struggle and my endeavors against the multitude of organizations and people that would like to prevent this information and data from coming to light. I am honored to be able

to demonstrate and prove with evidence and irrefutable data that our work is paramount to the cyber security of a company, an organization, a U.S. State, a Nation, and the World.

I will explain why the current cyber security posture is in a critically vulnerable position (Code red) for the entire Alaskan State Government and requires immediate remediation and addressing. Alaska has been repeatedly attacked by so called, highly sophisticated cyber criminals, possibly from adversary Nation States. We are aware of four (4) reported cyber attacks. Three (3) of which have occurred after our initial intelligence and sharing of the insecure infrastructure with numerous known and available attack vectors. Two (2) cyber attacks, the voter website and the Courts were warned as vulnerabilities by us prior to the attacks

9:13:11 AM

MR. STEPHENSON provided his personal background. He said he is a U.S. Army veteran with top security clearance. He has worked within the North Atlantic Treaty Organization (NATO). While in the US Army he served in the National Security Agency. His cybersecurity training started with the Rainbow Books, which is a series of computer security standards developed by the U.S. Department of Defense (DoD) in the 1980s and 1990s. After leaving the US Army, he became a DoD contractor in the United Kingdom (UK) at an intelligence gathering center for Europe. His understanding of cybersecurity and data manipulation was enhanced with this assignment. After that he moved into vendor and partner solutions as a lead engineer and became familiar with many different companies and the solutions they offer.

MR. STEPHENSON related that for the past five years he has focused on cybersecurity, working with a technology developed inside NATO called "truth serum." This work uncovered a Stuxnet [a malicious computer worm], like a malware solution inside NATO. This tool also uncovered ways that the Chinese were attempting to steal data from the Joint Strike Fighter (JSF) program. He said he mentioned this because several slides in the presentation show technology the Chinese have stolen through various DoD contractors and allied partner nations. He said this work has helped him focus his discovery skills to identify the penetration access points on public-facing internet infrastructure.

9:18:25 AM
MR. STEPHENSON said cybercriminals use websites and public-facing infrastructure vulnerabilities for their initial access. Once inside, they work to achieve elevated access before running a malware or ransomware attack. He now ranks the attack vectors from 1-10 or low to critical, based on national and international industry standards.

9:20:13 AM
MR. STEPHENSON paraphrased the four known Alaska cyberattacks described on page 3 of the presentation, which read:

[Original punctuation provided.]

> **1st Cyber Attack:** 26th April 2018. Alaska's Division of Public Assistance (DPA), a department in Alaska's Department of Health and Social Services (DHSS) was breached with a trojan virus. It exposed more than 100,000 Alaskan citizen's Personal Identifiable Information (PII). It was also found to be noncompliant with the Health Insurance Portability and Accountability Act a.k.a. HIPAA.
>
> - https://www.manageengine.eu/log-management/data-breaches/alaska-households-cyber-attack.html
>
> **2nd Cyber Attack:** September 2020. Alaska State Government's voter registration website was breached exposing again the PII of over 113,000 Alaskan citizens. This breach was announced in late November 2020.
>
> - https://www.manageengine.eu/log-management/data-breaches/alaska-households-cyberattack.html
> - In May 2020 we notified Alaskan Government representatives that this website was critically vulnerable and needed immediate attention after having assisted the FBI with a similar security issue with the Central Voting system (www.vote.gov) redirecting to a Korean DNS.
> - This Actionable Intelligence was acknowledged; however, we were informed that the State of Alaska would not be engaging at that time. This was due to the recent COVID Pandemic and the subsequential knock on effects to Alaska.

    - We understand that statement, however, question the rationale. In our vast professional experience, these exposed cyber vulnerabilities act like beacons to cyber criminals.
- To ignore a warning of cyber insecurity is foolish and unsafe. Failing remediation could constitute being complicit by being complacent, or even negligent - especially when the person, or persons informed include Chief Information Security Officers (CISOs) and any Chief Officers (CxO) or Board Member.
- The insecurity across the country is systemic and not confined to a single sector, but all sectors including Banks, Healthcare, and Insurers, just to name a few.

9:24:25 AM
MR. STEPHENSON continued to paraphrase the known Alaska cyberattacks described on page 3 of the presentation, which read:

[Original punctuation provided.]

> **3rd Cyber Attack:** April 2021-Malware was placed on Alaska's court system email.
>
> - On 1st April 2021 I emailed the Alaska state Attorney General and the State Governor. A copy of this email is included for reference in Appendix [D]. Please note in the bulleted section of warnings of vulnerable web site, I specifically identified the Alaska Courts website. This item is highlighted for referencing purposes.
>
> **4th Cyber Attack:** Breached in May 2021-The Department of Health and Social Services (DHSS)

MR. STEPHENSON said the only response he received from the Alaska government was in early May 2020, indicating they did not want to engage. A copy of the email is included in Appendix D of this report.

9:25:57 AM

MR. STEPHENSON paraphrased page 4 of the presentation, which read:

[Original punctuation provided.]

9:25:58 AM

Even though the data and warnings that have already been provided to the State of Alaska shows a systemic lack of cyber security, in preparation of this statement, I wanted to have a more up-to-date and deeper understanding of the cyber posture for Alaska's Government. My preparations initially uncovered ninety-eight (98) Government websites including twenty-two (22) main Government Departments, and organizations linked to the Alaskan Government. One example of an organization is the Alaska Energy Authority. These organizations have a .org and not a .gov ending on their website and domain name but are still linked via Alaskan Government websites.

9:27:04 AM

As a cursory check I accessed each of the main Government Department websites just as any normal person would using a standard web browser. I did this to confirm that these websites were active and accessible. Of the twenty-two (22) Government Departments, eight (8) were 'Not Secure'. That is one-third (1/3) of the official webpages for the Alaskan Government Departments have cyber security issues rendering them not secure. These not secure websites include:

- Alaska State Legislature
- Department of Military and Veterans Affairs - Division of Homeland Security Amber Alert
- Alaska Court System
- Department of Natural Resource
- Department of Natural Resources - Division of Forestry
- Department of Law
- Regulatory Commission of Alaska
- Department of Revenue - Tax Division

MR. STEPHENSON said he circled items in the presentation in red to highlight that the website is not secure.

9:27:51 AM
MR. STEPHENSON paraphrased page 5 of the presentation, which read:

[Original punctuation provided.]

> A website can be considered 'Not Secure' for many reasons. In July 2018, Google made an update to its browser to include a "Not Secure" warning in the address bar as shown circled in red in the above screenshots. This means that the website is not using a secure connection, meaning that the data being transferred, viewed, and entered is not encrypted. A not secure warning can result for many reasons. Some are misconfigurations that can quickly be fixed, others are more serious including issues with the encryption or the encryption certificate and keys being, or sometimes not being used. This action was initiated by Google, as stated, in 2018, in hopes to help promote secure encryption connections ensuring that the data being used and in transit on the internet is encrypted. Sadly today, 3 years later, this is an obvious configuration missed by many, but capitalized upon by cyber criminals.

9:29:09 AM
MR. STEPHENSON continued to paraphrase page 5 of the presentation, which read:

[Original punctuation provided.]

> I wanted to investigate the presence of additional Alaska subdomains to gain an understanding of the scope of the Alaskan Government websites and presence on the internet. This took me to the first of the recently discovered ninety-eight (98) websites listed in alphabetical order, www.akenergyauthorty.org. A great example and opportunity to look at exactly what an organization under the Alaskan Government might look like. Unfortunately, this immediately started with a "Not Secure" website as shown in the screenshot below. It also identified an additional six subdomains now taking total websites needing to be investigated for cyber security to one hundred and four {104). In addition, two of the subdomains had an additional open port, and the server hosting the website had two

additional open ports, four ports in total, that will each require further ingestion.

9:30:51 AM
MR. STEPHENSON continued to paraphrase page 5 of the presentation, which read:

[Original punctuation provided.]

I decided to take an initial Cyber Rated Index (CRI) score of the Alaska Energy Authority website. This is where the cyber security posture started rapidly spiraling into critical. As shown in the picture below there are critical cyber security issues with the Public Key Infrastructure (PKI) certificate used on the website, 4 Common Vulnerabilities and Exposures (CVEs) all with a MEDIUM risk rating per the Common Vulnerability Scoring System (CVSS) version 3.1, and additional cyber security vulnerabilities identified elevating this website and organization to a critical cyber security risk. In other words, a CRI score of F (FAILURE).

9:31:28 AM
SENATOR KAWASAKI joined the meeting (via teleconference).

9:32:15 AM
MR. STEPHENSON referenced the picture on page 5 and explained that the Public Key Infrastructure (PKI) certificate shown has a 10-year lifespan and will not expire until 2027. This is despite the fact that best practice and the industry standard for a PKI certificate is a maximum of three years, but PKIs are often limited to months. He highlighted that if cybercriminals gain access to an organization and have obtained a PKI certificate, they want the longest certificate lifespan to avoid requesting a renewal. Simply because the PKI certificate shown has a long lifespan does not mean a cybercriminal has access, but it is indicative of cybercriminal activity. He noted that he works with one of the largest IT and cybersecurity providers in the world that recently discovered a website with cybercriminals lying in wait, gaining privileges similar to what happened with the SolarWinds attack. The PKI certificate hides cybercriminals, but he is able to find them and investigate them further. He acknowledged that a PKI certificate may not be indicative of cybercriminal behavior, but it should be investigated.

9:34:44 AM

MR. STEPHENSON mentioned the four common vulnerabilities or CVEs listed in the photo on slide 5 [Original punctuation provided]:

- 4 Common Vulnerabilities and Exposure (CVEs) - all MEDIUM RISK
- Failed every data protection law, regulation and standard, GOPR, PCI, DSS, HIPAA, NIST, etc.
- Website does not redirect HTTP to HTTPS ensuring website security (i.e., NOT SECURE)
- Addition open ports
- Potentially managed by a 3rd party - General Communications, Inc. in Anchorage, Alaska

9:34:49 AM
MR. STEPHENSON said that once a vulnerability is announced publicly, the company creates a common vulnerability and exposure and assigns a numeric to that vulnerability and provides a patch. He clarified that every CVE he cites is known and exploitable. If it exists on a system, it can be actively used by cybercriminals to gain access.

9:35:29 AM
MR. STEPHENSON noted that he also mentioned that the website failed data protection laws and regulations, specifically, Europe's general data protection requirement regulation. The Payment Card Industry Data Security Standard (PCI DSS) for banking, healthcare HIPPA, and the National Institute of Standards and Technologies (NISTs). Furthermore, the website did not redirect from http. He explained that when a user accesses a website through a browser, there are two ports: http and https. The unsecured http port presents information to the browser, which was the web interface started years ago. The secure https port has since been incorporated. Http is typically assigned port A and https is assigned port 443 on a server.

9:36:29 AM
MR. STEPHENSON stated that he always advises turning off the http port A because there is no reason to have an unsecure protocol open. But what he discovered is not only were both ports open, but if he asked his browser to access the website over the unsecure http, it would not redirect to the secure https. All data on that unsecure site is viewable by anybody, he said.

9:37:27 AM

MR. STEPHENSON directed attention to the screenshot on page 6 of the cyber rated index of the legislative website. The results were checked again just last night to confirm these findings. He said he would explain the security vulnerabilities later in the presentation.

9:38:00 AM
MR. STEPHENSON turned to page 7 and paraphrased the conclusion, which read:

[Original punctuation provided.]

> **CONCLUSION**
>
> The cyber security posture of the Alaskan State Government is not an anomaly. Unfortunately, we experience many similar cyber postures in many organizations and industries, including the very IT and cyber security vendors in which rely upon daily. I have additional information that I have prepared for you in this brief.
>
> They are:
>
> - **Appendix A:** pg.8 - The initial Cyber Rated Index (CRI) report I provided to Alaskan Senators just last month
> - **Appendix B:** pg. 16 - Excerpt of email sent on 9th April 2020 warning of elections website
> - **Appendix C:** pg. 18 - Excerpt of email sent on 30th May 2020 to Commissioner at Alaska Department of Administration
> - **Appendix D:** pg. 19 - The email to Alaska's Attorney General warning that the Alaska Court system was vulnerable, among others
> - **Appendix E:** pg. 21 - Weaponizing of the internet
> - **Appendix F:** pg. 23 - Lack of cyber security with IT and Cyber vendors
> - **Appendix G:** pg. 25 - Where to go from here?
> - **Appendix H:** pg. 26 - Additional Information and References - third party professional reports validating the critical necessity to ensure cyber security to public facing internet webpage infrastructure
> - **Appendix I**: pg. 28 - Partners

9:40:03 AM
MR. STEPHENSON continued to paraphrase page 7 of the presentation, which read:

[Original punctuation provided.]

> There is one connection that I would like to highlight between Appendix E: Weaponizing of the internet and Appendix F: Lack of cyber security with IT and Cyber vendors. In Weaponizing of the internet, I briefly cover STUXNET and how unknown Microsoft zero-day vulnerabilities were utilized to gain initial access. Now I want to correlate that to the information in Appendix F where I briefly cover SolarWinds, codenamed SUNBURST. Senators and Representatives, understanding the direct connection between these two are paramount to understanding the problem.

9:40:38 AM
CHAIR SHOWER interjected to relay a request the committee move into executive session because of the sensitivity of the topic. He advised that he had instructed his aide to contact Legislative Legal Services for clarification.

CHAIR HOLLAND said he was not overly concerned because much of this information is already available to the public, but he would like to hear from Legislative Legal. He suggested that the committee take a short break and noted that a text thread was running among the committee members. He asked Mr. Stephenson if he had anything to add.

9:43:12 AM
MR. STEPHENSON confirmed that he was accessing the legislative system through a web browser interface. He found vulnerabilities and if he could find them, so can cybercriminals. Nevertheless, he agreed with Senator Shower that it is not wise to speak publicly about vulnerabilities. He noted that because of the sensitivity of the topic, he only invited Mark Sayampanathan to join this briefing.

9:44:28 AM
At ease

9:54:40 AM
CHAIR HOLLAND reconvened the meeting and advised Mr. Stephenson to disconnect from the Teams meeting and call the 800 number,

844-586-9085, since the committee plans to go into executive session.

9:56:38 AM
SENATOR HUGHES asked for the number and Chair Holland repeated it.

SENATOR SHOWER clarified the area code.

9:57:42 AM
SENATOR KIEHL pointed out that in executive session the committee could only discuss the things that present a great threat to the state. Thus far, the presentation has only covered general cybersecurity items and those topics cannot be discussed in executive session. He cautioned the committee to be careful about how it splits the conversations because a substantial amount of the information would be appropriate for the public session. He acknowledged that it would be difficult for the chair to decide how to split the topics.

9:58:32 AM
CHAIR HOLLAND asked Mr. Stephenson whether the committee should move into executive session immediately.

9:59:05 AM
MR. STEPHENSON replied his intention was to discuss the vulnerabilities of the Alaska Legislature's website in addition to some of the others he previously mentioned. He offered to tailor his comments to cybersecurity for Alaska.

9:59:40 AM
CHAIR HOLLAND clarified that there would be no votes taken during this meeting or while the committee is in executive session. This is a presentation so legislation was not being considered.

10:00:07 AM
SENATOR HUGHES asked if it would be appropriate to have Tim Banaszak, the Information Technology Manager, participate if the committees will go into executive session and discusses the Alaska State Legislature website in particular.

CHAIR HOLLAND offered his belief that it would be appropriate.

10:00:30 AM
MR. STEPHENSON advised that he planned to discuss the weaponizing of the internet as well as the lack of cybersecurity

with IT and cyber vendors, neither of which correlate directly to the Alaska government. He said he could either go over those now or leave it to the members to read in the report. He proceeded to explain that the weaponizing of the internet explains how the U.S. and Israeli agencies developed a code for Stuxnet [malware to adversely affect an Iranian nuclear facility]. It used a Microsoft vulnerability zero day for access. Stuxnet showed the world that the internet can be used for cyberwarfare.

10:01:40 AM
MR. STEPHENSON noted the two screen shots of the U.S. joint strike fighter and the Chinese passenger airliner on page 22 reference the technologies that have been stolen through cybertheft. He described the way this correlates to the State of Alaska:

> Think of SolarWinds. They had supply chain into tens of thousands of companies because they provided a solution. So every IT cybersecurity hosting whatever vendor the State of Alaska uses, is inherently a supply chain vulnerability being brought in, making your government insecure. And that's how I tie those two together.

10:02:38 AM
SENATOR KAWASAKI offered his view that much of this information is available online and that it should be presented to the entire legislature rather than in executive session to just these two committees.

10:03:28 AM
SENATOR HUGHES offered her understanding that any legislator could call and join the executive session.

10:03:54 AM
SENATOR KAWASAKI restated his position.

10:04:30 AM
MR. STEPHENSON interjected to explain that he uses open-source intelligence (OSINT) available on the internet. He described it as the interactions of the computers interfacing with web pages and the browser. OSINT uses information that is publicly available to anyone. However, this does not mean that people have the ability to decipher the information or determine existing vulnerabilities.

10:05:20 AM
CHAIR HOLLAND expressed doubt that 60 legislators could be convened via telephone in the next hour to listen to the presentation.

10:05:51 AM
CHAIR SHOWER stated that Megan Wallace, Director of Legislative Legal Services, was available to advise the committee.

10:07:10 AM
CHAIR HOLLAND recognized Megan Wallace.

10:07:15 AM
MEGAN WALLACE, Director, Legislative Legal Services, Legislative Affairs Agency, Alaska State Legislature, Juneau, Alaska, stated that it was brought to her attention that the committee wants to discuss cybersecurity issues that may potentially affect the security of state agencies. She cited Uniform Rule 22(b) and recommended, in conjunction with advice from Tim Banaszak, that these discussions be held in executive session. She added that while there may be interest at some point in briefing another group of legislators or the public on the issues that will be considered, her recommendation is to delay that until after there has been a more deliberative process of assessing the risks.

10:08:55 AM
CHAIR HOLLAND summarized his understanding of her recommendation.

10:09:25 AM
MS. WALLACE explained that it is difficult to give comprehensive advice without knowing the matters that would be discussed out of executive session versus in executive session. Based on her understanding of the information that will be presented, her recommendation is to hear it in executive session.

10:10:00 AM
At ease

10:11:37 AM
CHAIR HOLLAND reconvened the meeting and advised that Mr. Stephenson would speak on the non-sensitive issues he previously mentioned. At that point then the committee would move from Teams to the phone lines for an executive session.

10:12:14 AM

CHAIR SHOWER agreed with the plan to listen to less sensitive topics before moving into executive session.

10:12:39 AM
CHAIR HOLLAND asked Mr. Sayampanathan to put himself on the record. He stated the committee was having audio issues.

10:13:04 AM
MARK SAYAMPANATHAN advised that he was unable to participate in the chat committee members were having.

10:13:22 AM
At ease

10:14:14 AM
CHAIR HOLLAND reconvened the meeting.

10:14:21 AM
SENATOR HUGHES pointed out that whoever was controlling the livestream through AKL.TV is not supposed to stream when the committee is at ease. She asked if streaming is occurring during the committee at eases.

10:14:38 AM
CHAIR HOLLAND agreed that when the committee is at ease the broadcast should stop. He recommended that the committee exercise caution. Seeing no further questions or comments from the committee, he asked Mr. Stephenson to continue.

10:15:10 AM
MR. STEPHENSON paraphrased his conclusion on page 7. He recapped that his intent was to draw a correlation between weaponizing the internet, including brief coverage of Stuxnet, how unknown Microsoft zero-day vulnerabilities were used to gain the initial access, and the information in Appendix F that briefly covers SolarWinds, code name SUNBURST. Understanding the direct connection between these two is paramount to understanding the problem, he said.

10:15:50 AM
At ease

10:16:39 AM
CHAIR HOLLAND reconvened the meeting and asked Mr. Stephenson to resume.

10:17:09 AM

MR. STEPHENSON continued to paraphrase the conclusion on page 7 of the presentation, which read:

[Original punctuation provided.]

> Understanding the problem means steps can be taken to mitigate the problem. The connection I would like to make clear is that the same methods of exploitation and manipulation that were used by the agencies in STUXNET were also used in SUNBURST. These methods are being used daily against companies and governments to devastating effect.
>
> To close my opening statement, and before I dive into the data and examples, I would like to re-read my opening statement as now the clarity and understanding of that statement should ring true and act for the urgent call to arms before the next attack on the Alaskan State Government undoubtedly occurs.
>
> "The State of Alaska has suffered 4 separate cyberattacks in less than 2 years. We have been informing and providing evidence directly to Alaska over the last 18 months of why. This is because Alaska's current IT and cyber vendors are NOT providing adequate protection, and Alaska's IT infrastructure is Insecure. This is an obvious statement, unfortunately what we see every day is that the obvious is constantly being overlooked."
>
> Inaction will not fix the problem nor make it go away, it will simply compound the challenges and costs. Ensuring voting integrity is critical to our Democracy. Senators, we stand ready for service.

10:19:13 AM

MR. STEPHENSON directed attention to Appendix E on page 21 of the presentation. He paraphrased Appendix E, which read:

[Original punctuation provided.]

> **APPENDIX E: WEAPONIZING OF THE INTERNET**
>
> The age of the computer and the internet has developed and rapidly advanced science and technology for the benefit of the world, the United States, and the State of Alaska. One such amazing example is the accelerated

advancements in the medical field. This computer age has also seen the accelerated growth and reliance on IT systems in our daily lives. It has brought about the internet and the ability to share and use information open and freely in seconds to anywhere in the world. It has provided the ability to have live video chats, like the one we are on today. Compared to just 20 years ago this was practically impossible and required either telephone, satellite link or travel.

In all the immense benefits this has brought, it has also created the weaponization of the same internet. The first real display of this weaponization occurred with the STUXNET malware used to cause catastrophic effect on the Iranian Nuclear Facility. STUXNET was first discovered in 2010. That is only 11 years ago. It was developed to attack targeted programmable logic controllers (PLCs) manufactured by Siemens that are used to automate machine processes specifically those in Nuclear Facilities. It is now widely accepted that STUXNET was created by the intelligence agencies of the United States and Israel. So, we have basically created our own worst nightmare.

10:21:45 AM
MR. STEPHENSON continued to paraphrase Appendix E of the presentation, which read:

[Original punctuation provided.]

One fact about STUXNET that is particularly interesting is that it exploits multiple previously unknown Windows zero-day vulnerabilities to infect computers and spread. Does that ring a bell for anyone? Just this past month there have been a number of newly identified Microsoft zero-day vulnerabilities including the Autodiscover vulnerability. What makes the Autodiscover vulnerability particularly bad is not the fact that it is a serious attack vector that cyber criminals can and have used, but the fact that Microsoft was aware of this vulnerability for 5 years.

Reference: Article published on 27th September 2021 by the Register states how Microsoft knew of the Autodiscover vulnerability 5 years ago.

https://www.theregister.com/2021/09/27/microsoft exchange autodiscover/

10:22:59 AM
MR. STEPHENSON continued to paraphrase Appendix E on page 21 of the presentation, which read:

[Original punctuation provided.]

> We can also learn a lot from the unfortunate and treasonous release of the thousands of classified documents by Edward Snowden in 2013. Some of those documents included classified briefing documents from the National Security Agency (NSA). They explain the ability that the United States had to take control of IT systems even after a fresh and new installation of software and firmware. What we discern from this is that the United States had these capabilities before the Snowden debacle in 2013. What this again reaffirms is the complete insecurity of every connected system, especially everything that is Information Technology.

10:24:06 AM
> From 2010, to 2013, and fast forward to 2021, Alaska's Government, just like all U.S. State Governments, implemented and became dependent on IT systems throughout every department, organization, district, and incorporated town. All the Personable Identifiable Information (PII) and other data considered to be sensitive or classified has been consolidated and stored on IT systems, clouds, databases, and such. This wealth of information is invaluable to criminals for a multitude of nefarious purposes.

10:24:54 AM
MR. STEPHENSON reviewed the examples on page 22 of the presentation, which read:

[Original punctuation provided.]

> Cyber Threats That are NOT Caught or Prevented by Other Solutions
>
> If there were others then these and many other cyber intrusions, attacks, etc., would have been prevented
>
> - https;J/www.cnbc.com/2011/11/08/chinese-theft-of-

sensitive-us-military-technolOft:Still-hua-problem.html

- China builds the J-20, a new stealth fighter jet, they were reportedly helped by industrial espionage. The design resembles the F-22. And the FC-31 Gryfalcon, in development, resembles the Lockheed F-35 Joint Strike Fighter
- "What Beijing has been very good at Is targeting U.S. defense contractors, getting Into their computer systems through various types of essentially c:yber warfare and steaUngthe designs of some of America's best military assets: said Harry Kezlanls, director of defense studies at the Center for the National Interest, a think tank founded by former President Richard Nixon.
  - According to Kazlanls, the Chinese have been able to hack into computer networks to steal designs and other Information on U.S. carriers, advanced defense systems as weH as the F-22 and F-35 jets.
- https·IIJNww,claHyman co ykfscJencetecbllflde;-389312§/Chlnese:A: 2fl-stealth-jet-baR4::rnlljtaCY::Qlanwtplen-haclcpl'5;;mafres:pubHc- d@byt html

10:26:02 AM
MR. STEPHENSON reviewed the second example on page 22 of the report, which read:

[Original punctuation provided.]

- https://www.extremetech.com/extreme/300313-report-chinas-new-comac-c919-jetliner-is-built-with-stolen-technology

MR. STEPHENSON stated that the new Chinese [C919] passenger [narrow body jet built by the Commercial Aircraft Corporation of China (COMAC)] has technology for parts and components stolen through various means including cyber theft. This photo shows components and the source of the stolen data.

10:26:25 AM
MR. STEPHENSON turned to page 23 of the report and paraphrased Appendix F, which read:

[Original punctuation provided.]

APPENDIX F: LACK OF CYBER SEUCITV WITH IT AND CYBER VENDORS

> The level of lacking cyber security is systemic across our IT and cyber security vendors that we use and rely on every day. I have personally researched over 150 of the top IT and cyber security vendors and manufacturers. The systemic lack of fundamental cyber security across their plethora of internet facing websites, domains and subdomains is a standing example of the lack of knowledge and expertise, by these very professionals, to close the initial access points used by cyber criminals.

10:27:12 AM
MR. STEPHENSON described a discovery he made last week. He said he looked into a main IT provider in the U.S. based on information he had seen on the internet. He discovered that one of their VPNs had expired PKI certificates that were running encryption algorithms that can be hacked in 6-10 minutes. He notified the vendor of his findings but ultimately the provider decided not to proceed. Unfortunately, in his view this is the standard reaction, he said.

10:28:18 AM
MR. STEPHENSON returned to the report on Appendix F on page 23 of the presentation, which read:

[Original punctuation provided]

> Take for example the SolarWinds breach. This well-known cyber attack and breach was an amazing example of the cunning, patience, and skill that we face in today's cyber criminal. This breach alone has affected over 18,000 companies worldwide including the U.S. Federal Government and Department of Defense. The cost of the cleanup of this one single attack is estimated in the $billions.

10:28:51 AM
> This attack was so prolific and damaging that it caused the United States Senate to conduct a hearing dedicated to understanding how and why this took place. Testimonies were heard from some of the Chief Executives and cyber experts from many professional and top tier cyber companies including SolarWinds

themselves. They answered many questions posed by U.S. Senators; however, the absolute single and most important question was never asked by anyone, not a Senator, not an investigator, no one. That one question is: How did the cybercriminal(s) gain the initial access into SolarWinds?

10:29:38 AM
MR. STEPHENSON continued to review Appendix F on page 23 of the presentation, which read:

[Original punctuation provided.]

While the SolarWinds cyberattack was sophisticate in the total scope, the initial access was not. It was simple. It was not by any means sophisticated. It was a website that the cyber criminals were able to breach and spoof. This got them inside the infrastructure of SolarWinds and allowed the criminals to move internally undetected for months.

The cyber criminals gained access to SolarWinds by exposing readily available cyber security vulnerabilities on their public facing internet webpages and infrastructure. Just like the ones in Alaska's Government. The cyber criminals were able to create a duplicate website with a different URL, but a website that looked identical to an official SolarWinds website. This tactic is called website spoofing. They were then able to exploit the known and readily available vulnerabilities on their internet systems to gain access, eventually attaining administrative access. Once they had this, they were able to use the SolarWinds IT systems to assign a real PKI encryption certificate to their spoofed website giving the website the added appearance of being a valid SolarWinds website. From there the criminals used their time and privileged access to move laterally within the company and insert malicious code into an update of the SolarWinds software that would eventually be pushed out to their customers.

10:31:47 AM
MR. STEPHENSON continued to paraphrase Appendix F on page 23 of the presentation, which read [Original punctuation provided]:

So why was this question never asked, or answered in this emergency U.S. Senate hearing?

10:32:00 AM
Microsoft was notified by us in August 2019 about the existence of hundreds of security flaws in the CRYPT32.DLL. One of Microsoft's API modules. This security flaw was discovered by us using Whitethorn. We contacted Microsoft and disclosed the information pertaining to the security vulnerability. Microsoft performed their own internal research to try to discover this vulnerability and were unable. After their response back to us stating that they were unable to locate the vulnerability we replied with further information on the vulnerability and how to identify it. Again, Microsoft was unable to locate the vulnerability. In the end it took us hand-walking their cyber security 'experts' through the discovery of the vulnerability that resulted in the patch and announcement of CVE- 2020-0601 for Windows CryptoAPI Spoofing Vulnerability. The severity of this vulnerability is rated as HIGH with a score of 8.1 out of a possible 10 according to National Vulnerability Database's (NVD) latest version, version 3.1. The National Vulnerability Database is a database maintained by the National Institute to Standards and Technology, a.k.a. NIST. NIST is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.

Reference: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

10:35:10 AM
MR. STEPHENSON continued to review Appendix F on page 24 of the presentation, which read:

[Original punctuation provided.]

What is worse. The updated version of the CRYPT32.DLL included a minimum of 4 embedded certificates, i.e., vulnerabilities. We know this because we scanned it with Whitethorn after its release. After the CVEs release the CRYPT32.DLL that was being used by ZenMAP (NMAP security scanner) utilized version 6 and held 379 certificates with the same spoofing capability.

A few months later Microsoft was again contacted by us because I had first-hand discovered critical vulnerabilities on their internet presence in Israel. At this time, we agreed to act in the best interest of

all and as conscientious cyber professionals proving the information to Microsoft. We all want to make the world and the internet a safer place, right? Microsoft took the information and were able to remove some of the most critical vulnerabilities that we identified. What remains puzzling to this very day is why Microsoft will not extend the same level of professionalism and engage us in discussions on the vast number of other internet vulnerabilities we have discovered and notified them about. To date, Microsoft continues to refuse to engage, and only try to push to their free disclosure program. They are not alone in this practice. Just last week an Apple iOS zero-day was released by a vulnerability hunter because Apple refused to responsibly engage with them and fix the vulnerability.

10:38:19 AM
MR. STEPHENSON continued to review Appendix F on page 24 of the presentation, which read:

[Original punctuation provided.]

The final example that I will provide demonstrating how rife the IT and cyber security industry is with cyber security vulnerabilities and their negligence to engaged will be an example using the zero-trust Rockstar Zscaler. Over the course of a few months, I compiled the Cyber Rated Index (CDI) scores of over 150 of the top IT and cyber security companies in the world. Zscaler was included in this compilation Scoring an F and having discovered a number of vulnerabilities that places the company's infrastructure and solutions at unquestionable risk - think SolarWinds.

10:39:44 AM
MR. STEPHENSON continued to review Appendix F on page 24 of the presentation, which read:

[Original punctuation provided.]

I contacted a previous co-worker, their vice president of Federal. He had an employee and mutual friend contact me. I provided information about the cyber security vulnerabilities and was given the contact information for a Mr. Desai, their CISO. Following our

conversation, I reached out directly to Mr. Desai on 22nd January 2021. He never responded that or any of my attempts to engage and help. Others that I work with, including the CEO Andy Jenkinson, who is also on this call, also reached out to a number of Zscaler's executives including their CEO. Not one response from all the attempted contacts and warnings we provided of insecurity, including noncompliance to data protection laws and regulations.

10:40:46 AM
MR. STEPHENSON said he mentions this because these are global companies that are in breach of data protection laws, including Europe's General Data Protection Regulation and California's Consumer Protection Act. These known vulnerabilities exist on their websites and infrastructure and their customers' data is vulnerable and exploitable by cyber criminals.

10:41:51 AM
MR. STEPHENSON directed attention to Appendix H on page 26 of the presentation to highlight Application Programming Interface and vulnerabilities, which read:

[Original punctuation provided.]

1. IBM Security: A recent report by IBM Security proving that two-thirds of all cloud based cyber attacks originate through insecurities (misconfigured APIs) on the public facing internet webpages, domains, and IT systems.
   a. https://siliconangle.com/2021/09/16/ibm-report-finds-two-thirds-cloud-breaches-traced-miscon-figured-apis/

MR. STEPHENSON explained that an Application Programming Interface (API) is a software intermediary that allows two applications to communicate with one another. One problem with APIs is the vulnerabilities provided. For example, files can be added and deleted on the server at the location of the URL. This illustrates the potential for malicious code entries through APIs.

MR. STEPHENSON referred to the second item in Appendix H on page 26 of the presentation, which read:

[Original punctuation provided.]

2. HackerOne: 2021 Hacker Report showing 96% of all hackers are working on websites

10:43:42 AM
MR. STEPHENSON explained that the use of "hacker" doesn't necessarily mean "bad guys." This report identifies websites as the biggest risk for breaching. APIs and Android applications can be breached because people access websites while using their devices. Further, operating systems are affected since servers use the iOS to host the websites. These things cumulatively show why the public-facing internet is constantly overlooked for other penetration solutions.

10:44:36 AM
MR. STEPHENSON directed attention to the third item in Appendix H on page 27 of the presentation, which read:

[Original punctuation provided.]

3.McAfee report referenced in a recent article by CSO Online stating how the initial infiltration of a highly sophisticated cyber attack carried out by one of China's APT groups originated through the vulnerabilities on the web servers.
a. https:llwww.csoonline.com/article/3633632/how-apts-become-long-term-lurkers-tools-and- techniques-of-a-targeted-attack.html

4. The Open Web Application Security Project (OWASP). A nonprofit foundation that works to improve the security of software. OWASP publishes a yearly 'Top 10' web application security risks to eliminate and provides information on cyber security risks and vulnerabilities.
a. https://owasp.org/www-project-top-ten/

MR. STEPHENSON stated that breaches to Solar Winds, Colonial Pipeline, Florida School District and health care attacks happened through the public-facing internet.

10:45:30 AM
MR. STEPHENSON directed attention to the fifth item in Appendix H on page 27 of the presentation:

[Original punctuation provided.]

EA Games breached through insecure cookies. Cookies play an important role in today's internet usage. They have been designed to help improve interaction with websites and can track, personalize, and collate, collect, and share Personal Identifiable Information (PII) about each user's session. Cookies can also be extremely dangerous as they can contain PII and data including login ID and passwords, as well as keylogging and other data entered on a website.

10:46:12 AM

An example on how critical a cookie can be is the recent breach of Electronic Artists (EA) Games. The hacker purchased login and password information from a cookie off the Dark Web for $10. They then inserted the cookie into an insecure, and exploitable subdomain and used this to obtain access to EA Games and steal the source code for the new FIFA 21 game.

MR. STEPHENSON said this concludes all of the non-Alaskan-specific information he planned to share today.

10:47:07 AM

CHAIR HOLLAND stated he appreciated Appendix G. He related his understanding that many of the cybersecurity problems are not with agencies such as the Alaska state agencies but with vendors using the IT system.

10:47:47 AM

SENATOR KIEHL asked if the hacks to the Alaska Division of Elections and the Alaska Court System were due to the vulnerabilities he identified.

10:48:07 AM

MR. STEPHENSON responded that he has not been engaged by the state so he could not specifically answer this. He said he was not a first-hand party to those cybersecurity breaks. However, he was aware of the vulnerabilities that would have allowed hackers to access the system.

SENATOR KIEHL recalled that he said the Stuxnet virus was introduced via the internet. He related his understanding that the two primary theories were that the virus was introduced by a thumb drive or early installation in the supply chain but not via the internet.

10:48:48 AM

MR. STEPHENSON answered that he was correct. He explained that he used "internet" loosely. He stated that they used Microsoft zero day vulnerabilities, which is across the internet. It was not specifically a direct attack.

SENATOR KIEHL explained the reason he asked was because he viewed the presentation as a slice of the broad topic of cybersecurity. Some things were not discussed, such as delivery by email, ransomware, or encryption issues. He asked what approach a large organization, such as state government should take with respect to cybersecurity.

10:49:51 AM
MR. STEPHENSON stated that he works for the Joint Analysis Center as a lead IT administrator for a couple of systems. IT typically divides up the responsibility into sections, including network, Windows, data storage or a specific email section. Thus, experts help manage the systems for each area. Cybersecurity experts must know everything, which is a daunting task. He stated his approach was to focus on a specific area of specific vulnerability. Cybersecurity has layers that all need to be protected. If the web interface is removed the site will be vulnerable regardless of inner protections. All of the hacks have resulted from vulnerabilities on the public facing internet.

MR. STEPHENSON highlighted that cybersecurity has many solutions. Cyber criminals look at three things. First, if the public face is exposed; second, their ability to access the site; and third, that since the face is not adequately protected, the inside is also not protected from the cyberattack.

10:53:13 AM
MR. STEPHENSON stated that criminals target any opportunity based on their open-source intelligence information gathered but not necessarily to target a specific group or organization. He said that his role is to eliminate the attack vectors to eliminate the opportunity to target an organization.

10:54:11 AM
SENATOR HUGHES recalled his opening remarks indicated that he warned the Division of Elections about cyberattack vulnerabilities. She said she has four questions. First, how far in advance of the election was the division warned. Second, what type of communication he used to contact the division and if it was by email and any response from them. Third, she asked if the

cyber criminals are able to detect his activity when he is checking and warning agencies, and if so, if they observe any precautions taken by the organization.

10:55:14 AM
MR. STEPHENSON responded that he was not sure if he should answer now or in executive session.

10:55:26 AM
CHAIR HOLLAND said he would leave it to his discretion but suggested he may wish to hold off and answer it during the executive session.

10:56:05 AM
MR. STEPHENSON answered that cyber criminals are not able to track his movements. He sends a request to the server who responds back with the capabilities. It provides a laundry list of information that provides him with the webpage and the infrastructure that he can click on and use. The information he uses is not trackable but there are organizations that report and openly track what other people use their tools to do.

CHAIR HOLLAND asked him to repeat his response as part of his response was inaudible.

MR. STEPHENSON said he responded to Senator Hughes' last question by saying that what he does cannot be watched or monitored on the internet because his action is with the server and the website. He acknowledged that there are organizations that do track tools others use but they do not track his movements.

He acknowledged there are a lot of solutions such as the cybersecurity "onion" model that focuses on one part but not the entire infrastructure.

10:57:21 AM
SENATOR KIEHL said there are never enough resources in corporations or government to meet the public's needs or wants. He acknowledged that the state would be more secure if it hired his firm and every other cybersecurity firm. He noted the precautions he takes at home, including a gun safe, and asked why the legislature should be concerned about its website and not focus on other things where there is personal identifiable information.

10:59:26 AM

MR. STEPHENSON responded that what he is presenting is not commonly implemented across the board. He stated his intention is to help, educate, and fix. He explained that he engages with professionals in every industry. Initially, the IT professionals are affronted by the information he provides.

10:50:26 AM
MR. STEPHENSON referred to the gun safe analogy and pointed out that the gun safe is locked, the front door is locked but some things are left outside. CIP could show you that your front door was left wide open and the safe is wide open in plain view. He offered his view that the importance to government is connected. Hackers breached SolarWinds at one location but it was not the attacker's end goal.

MR. STEPHENSON referred to his initial comments that highlighted that his firm has been tracking a cyberattack in progress. Just as at SolarWinds, the attacker spoofed the website, elevated their privileges and assigned a PKI certificate. This attacker is slowly finding where it wants to penetrate the system. An attacker's goal may not be the legislature although the attacker may use ransomware or encrypt the information it finds and sell it on the internet. However, their real interest may be to access other information it can find throughout the government infrastructure. It could get into critical national infrastructure such as power, water, and sewage. He said waiting gives them access through vulnerabilities. It is just a matter of time, he said.

11:01:15 AM
CHAIR HOLLAND stated his intention to take a short at ease to break the MS Teams links and then go to executive session.

11:02:22 AM
At ease for the committees to go into executive session.

11:59:47 AM
CHAIR HOLLAND reconvened the meeting and announced the committees were out of executive session.

12:00:21 PM
SENATOR HUGHES thanked the chair for the extended time for this hearing. The public heard the presentation at the beginning of the hearing, including that cybersecurity uses a different scale for grading. First, she asked if it was possible to raise a score of "F" to an "A." Second, she asked if he has raised any government's score. Third, she asked if there is any best

practice for state government portals for reporting and to ensure review of any warnings issued. She acknowledged that he wrote to the Alaska attorney general since cyberattacks can be criminal by nature. She wondered if someone familiar with cybersecurity would be a better point of contact.

12:02:13 PM
CHAIR HOLLAND asked if Mr. Stevenson was still available.

[An unidentified person commented that Mr. Stephenson was in the process of rejoining the teleconference].

12:02:28 PM
MR. STEPHENSON advised that he didn't hear the question.

12:02:41 PM
SENATOR HUGHES restated the question.

12:03:49 PM
MR. STEPHENSON answered no, he has not improved any state's cybersecurity but he has done so with other organizations and companies. As the legislature's IT manager stated, all of the findings must be analyzed. Each entity must assess the threat. Each entity's website is different. Typically, CIP would work with IT teams to provide solutions.

12:04:47 PM
MR. STEPHENSON said the second question is difficult since a lot of companies offer cybersecurity solutions. He said the cybersecurity community is large. He commented that IT personnel could spend all their time listening to people present their solutions to issues. He currently works as a freelance consultant for Cybersec but he works for other companies, too. He presented data based on Cybersec's interactions with the webserver. If you have a process it can help. He acknowledged the need for checks and balances to cut through the chaff to get to the valuable information. He suggested that this is something that should be addressed within the IT infrastructure.

12:06:50 PM
CHAIR SHOWER reminded members that this information is not confidential and the legislature is not breeching security by meeting to discuss how to improve security to thwart cyberattacks. The value of this meeting is to identify how vulnerable the state is to cyberattacks. He recommended that the state devote whatever time and financial resources are necessary to address cybersecurity since the state has been hacked. Those

cybersecurity breeches could result in data mining. He said the third largest economy on the planet is cybercrime, which affects businesses, government and individuals. He remarked that reviewing agency security measures is not meant to blame agencies for not doing a better job but to identify any weakness and correct them. He characterized it as a continual battle to "defend your castle." He viewed this as the beginning step.

12:09:58 PM
MR. STEPHENSON said he appreciates when people listen. He offered to assist the committee.

12:10:32 PM
CHAIR HOLLAND commented that it would likely take time, money and expertise to address cybersecurity.

12:11:11 PM
There being no further business to come before the committees, Chair Holland adjourned the Senate State Affairs Standing Committee and Senate Judiciary Standing Committee meeting at 12:11 p.m.