Idaho Technology Authority (ITA)

March 31, 2021 Approved Meeting Minutes

ATTENDANCE

Members Present:

Jeff Weak, CHAIR, Office of the Governor
Lori Wolff, Dept. of Health & Welfare
Brett Richard, Dept. of Labor
Charlene McArthur, Idaho Transportation Dept.
Maj. Bill Gardiner, Idaho State Police
Michele Tomlinson, Dept. of Correction
Faith Cox, Dept. of Administration
Terri Kondeff, Legislative Services Office
David Fulkerson, Div. of Financial Management
Chris Campbell, State Board of Education
Ben Call, Military Division
Greg Zickau, Office of IT Services
Wilma Robertson, IGC-EC Chair
Rep. Chris Mathias, Idaho Legislature

Members Absent:

Joshua Whitworth, State Controller's Office
Sen. Kevin Cook, Idaho Legislature
Kevin Iwersen, Idaho Supreme Court

Others Present:

Kristin Bartz, Office of IT Services
Mary Frances Coffman, Office of IT Services
Mark Mayer, Office of IT Services
Lance Wyatt, Office of IT Services
Brigette Teets, Office of IT Services
Keith Tresh, Office of IT Services
Matt Aslett, Office of IT Services
Sam Montiel, Office of IT Services
Chris Smith, Office of IT Services
Adam Warr, Attorney General Office
Alberto Gonzalez, Idaho Transportation Dept.
Bob Ross, Dept. of Fish & Game
Brett Richard, Dept. of Labor
Brian Reed, Idaho Transportation Dept.
Colby Austin, Dept. of Labor
Decar Scaff, Dept. of Education
Dylan Baker, Commission for Libraries
Faith Cox, Dept. of Administration
Holly Suit, Access Idaho
Jim Byrne, Lumen
Jeff Walker, Access Idaho
Josh Stemp, Idaho Transportation Dept.
Larry Sweat, PERSI
Mark Gosswiller, Dept. of Labor
Mark McKinney, Idaho Transportation Dept.
Mike Langrell, Idaho Military Division
Morgan O'Brien, Accenture
Matthew Thueson, Cradlepoint
Shannon Vihlene, Idaho State Historical Society
Sean McGillagreen, VMWare
Tawna Chesnut, Historical Society
Chad Williams, Salesforce

CALL TO ORDER

Chairman Jeff Weak welcomed the committee and called the meeting to order at 1:31 pm. Roll call was taken and a quorum established.

DECEMBER 9, 2020 MINUTES

MOTION: Mr. Greg Zickau moved and Ms. Charlene McArthur seconded a motion to approve the minutes of the December 9, 2020 meeting, as presented; the motion passed unanimously.

ITA SUBCOMMITTEE UPDATES

IT LEADERSHIP COUNCIL (ITLC) – Mr. Bob Ross, ITLC Chair, stated the committee has been busy but has no updates.

IDAHO GEOSPATIAL COUNCIL-EXECUTIVE COMMITTEE (IGC-EC) – Ms. Wilma Robertson, IGC-EC Chair, reviewed the results from the 2021 election. There are 16 members with four appointed position and 12 elected seats, and each year, half of the positions are up for election to serve a two-year term. This year, four seats were re-elected and the committee welcomed two new members, Eric Buehler with US Department of Agriculture, and Jeff May with Idaho Department of Fish and Game.

MOTION: Mr. Zickau moved and Major Bill Gardiner seconded a motion to ratify the results of the 2021 IGC-EC election; the motion passed unanimously.

ITA POLICIES

ITA Policy P5030 – GIS Framework Standards Development

Ms. Robertson reviewed the changes to the policy. A new process to develop, review, and approve GIS Data Standards was developed, which streamlines the creation and approval process, and removes redundant steps.

MOTION: Mr. David Fulkerson moved and Ms. McArthur seconded a motion to approved ITA Policy P5030; the motion passed unanimously.

ITA Policy P1010 – IT Policies, Standards and Guidelines Framework

Mr. Keith Tresh, Chief Information Security Officer for Office of IT Services, reviewed the changes to the policy. Definitions were moved to G105 – Glossary of Terms. Changed the two-year maximum implementation period to six months. This does not affect any current policies in creating unfunded mandates and agencies are able to take advantage of the exemption process if needed.

Mr. Ross noted this policy was edited and approved by ITLC but the policy before the committee is not the approved version.

Mr. Tresh apologized as the changes were made and it appears the wrong version was given to the committee.

Major Gardiner asked about the six month implementation period and whether this is an industry standard. Mr. Tresh responded this was a time frame agreed upon between the ITLC and the CISO office to ensure policies with a short time window, such as implementing cybersecurity policies, are addressed as quickly as possible.

Ms. McArthur asked for clarification on the time frames.

Chairman Weak tabled this policy until the next ITA meeting.

ITA Policy P1020 – Idaho.Gov Portal Privacy Notice

Mr. Tresh reviewed the changes to the policy. Definitions were moved to G105 – Glossary of Terms and fixed bullet numbering and formatting.

Mr. Ross noted this policy was also edited and approved by ITLC but the policy before the committee is not the approved version. Section IV under Policy, section numbers should read A through N.

MOTION: Ms. Robertson moved and Mr. Chris Campbell seconded a motion to approved ITA Policy P5030 as amended; the motion passed unanimously.

ITA Policy P2040 – Risk Assessment

Mr. Tresh reviewed the changes to the policy. Clerical updates were made to the abstract to align with the most current industry standard model. The definitions were also moved to G105 – Glossary of Terms. Mr. Tresh reminded the committee that per executive order, network penetration testing is already required to be conducted by all state agencies, so the requirement was further defined through a three-year plan in the policy. Results and corrective actions need to be forwarded to ITS CISO within 30 days of the test.

Mr. Fulkerson asked for clarification on the 30 day time frame and whether the requirement is for 30 days from the completion of the test or 30 days from the time the report is received from the third party tester. Mr. Tresh advised it is 30 days from the date the test results are received by the agency.

Ms. McArthur verified this is the version approved by ITLC. She further questioned some consistencies in language for large-scale projects. Asked about some definitions for project failure and major change of an IT project as defined in the policy. Ms. McArthur is concerned about the 30 day window to submit corrective

actions as it takes ITD a minimum of 60 days to get approval from their board. She is also concerned about the sequencing of events and would like agencies to be able to do their own assessment first, take corrective actions, then bring in a third party for the penetration testing to see how they are doing.

Mr. Tresh responded that the three year time frame is intended to be a cycle because they recognize that agencies will be at different stages. The intent is to ensure the third-party penetration testing is done at least once every three years as required by executive order. Mr. Tresh deferred on the definitions as those weren't changed in this modification.

Ms. McArthur recommended sending this back to ITLC to scrub the language for consistency.

Major Gardiner seconded what Ms. McArthur stated about the 30 days. Agencies with board oversight will have a difficult time meeting that requirement.

Ms. McArthur was further concerned about the exemption request process and the amount of paperwork that would cause. With the ITD board, items need to be submitted two to three weeks prior to the board meeting and then they take a 30-day review period, so it could be up to 90 days before they could get something submitted.

Chairman Weak agreed to send P2040 back to ITLC to clean up some of the details and add some language to delineate between agencies with and without boards as well as funding mandates.

Major Gardiner commented that 90 days should work for all agencies and the corrective action plan could outline any funding mandates that might need to be addressed.

Mr. Zickau agreed with cleaning up the language on P2040. He asked Mr. Tresh to clarify how this puts the Governor's executive order into policy and also to review the existing components of this policy agencies have already been operating under.

Mr. Tresh explained the 2017 executive order was renewed by Governor Little. It required penetration testing for all agencies but doesn't provide detail on how to conduct them. The modifications outlined in P2040 gives agencies guidance on how to do that and specifies using a third party in order to get a non-biased test. Agrees it would be reasonable to allow agencies 90 days from receiving the test results to submit. Mr. Tresh advised they did not touch the rest of the policy, just added the details for how the penetration testing should be conducted.

Mr. Zickau asked if the cybersecurity industry recognized self-testing as acceptable practice. Mr. Tresh replied that an internal testing is not acceptable for auditing requirements.

Ms. McArthur asked what is the difference is between a vulnerability assessment and a penetration test. Mr. Tresh replied that vulnerability assessments are an industry standard and should be on going within an organization. The penetration testing only needs to be conducted every three years.

Ms. McArthur inquired about the cost of testing. Mr. Tresh replied that ITS spent approximately $10,000 but it can range between $8,000 to $30,000 depending on the size of the agency.

Chairman Weak advised that funding for the penetration testing should already be included in each agency's budgets as it was added when the executive order was implemented. Mr. Tresh added that vulnerability assessments are generally included with penetration testing. Additionally, vulnerability assessments should be an ongoing practice with existing tools and resources.

Chairman Weak tabled policy P2040 until the next ITA meeting to allow ITLC to revisit issues addressed.

ITA Policy P4590 – Cybersecurity Incident and Breach Reporting Response Management
Mr. Tresh reviewed the changes to the policy. References to guidelines G525 and G585 were removed as they were both consolidated into standard S6010.

Mr. Ross noted this policy presented to ITLC. After some suggestions were made, the policy was withdrawn and the policy before the committee does not contain any of the edits suggested by ITLC.

MOTION: Major Gardiner moved and Mr. Zickau seconded a motion to approved ITA Policy P4590; discussion followed to consider P4590 together with Standard S6010 as they go together.

ITA Standard S6010 – Incident Reporting Handbook
Chairman Weak provided some background on this standard. Normally, ITA would not consider standards as they are approved at the subcommittee level. S6010 was not approved by ITLC and has been cleaned up with help from the technical working group and considered input from ITLC and stakeholders. Because of the importance of incident reporting and the need to update this standard, he made the decision to add it to the ITA agenda rather than wait for the next ITLC meeting.

Mr. Tresh reviewed the changes to the standard. After the last ITLC meeting, they met with the dissenting members to work through some of the issues. They corrected and updated the definitions for personally identifiable information (PII) to be consistent with Idaho statute. They addressed concerns that information was missing from incorporating G525 and G585 by auditing the information to verify nothing had been left out. There was only one section that did not get incorporated verbatim, which had to do with two processes – one for ITS customers and one for non-ITS customers. They also addressed concerns this standard would increase security requirements for existing systems, which is not the case. This standard addresses the process for incident reporting only. Accurate reporting is needed to be able to address cybersecurity threats to ensure the funding is in place and the focus is in the right place. To be able to do this, the statistics are needed from all agencies. The standard also clarifies that breaches are to be reported within 24 hours and incidents are to be reported within five business days, per statute and insurance requirements.

Ms. McArthur stated concerns about the incident reporting examples creating an unnecessary burden of reporting for her staff. Would also like the PII definition to be clarified.

Ms. Lori Wolff stated some of the same concerns about the PII definition and incident reporting examples.

Mr. Tresh advised that none of the Idaho statutes define personal information and not PII as defined by the federal government or National Institute of Standards and Technology (NIST). Mr. Tresh commented on the difference between a phishing email and a phishing campaign.

Ms. Wolff provided some clarification to their experience with PII issues when the state requirement was more stringent that the federal guidelines. They had to take some additional steps when going live with the vaccine website.

Mr. Fulkerson also had questions about phishing campaigns.

Mr. Chris Campbell pointed out the bullet numbers in the table of contents skips from eight (VIII) to ten (X). Mr. Tresh said they would look at that. Mr. Campbell also noted two statutes, Idaho Code § 33-133, which identifies PII for education, and Idaho Code § 18-31-22, which identifies PII in criminal code. Mr. Tresh indicated they would include those.

Ms. Faith Cox requested clarification for PII to include requirements for what constitutes a breach of PII since each component needs to be combined with another to be considered a breach.

Chairman Weak tabled standard S6010 until the next ITA meeting to allow ITLC to revisit issues addressed.

Major Gardiner withdrew his motion to approve policy P4590.

Mr. Fulkerson commented on the importance of this topic to move quickly and recognizes the need to send this back to ITLC to keep it at the top of the list. Cybersecurity issues are important to the bond agencies and other financial institutions as they frequently ask what the state is doing to address it to make sure they are protected. Mr. Ross advised the next ITLC meeting is in three weeks and will be able to get this addressed right away.

Ms. McArthur further added that cybersecurity is at the top of ITD's priority list, especially related to DMV data. She is focused on having her staff keep data safe and not pushing papers for exemptions and reporting just for the sake of doing work.

CYBERSECURITY TECHNICAL WORKING GROUP

Mr. Tresh provided the committee with information regarding the formal formation of an Enterprise Security Working Group (ESWG). The intent is to promote transparency with the governance and how to best manage the enterprise cybersecurity program. The membership would include all agency Chief Information Security Officers or their designee.

Although there has been a technical working group (TWG), research showed no formal formation of such a group within statute, charters, or through committee action. The ITLC has the power to form a TWG, staff could find no formal action taken by the committee to formalize the group. Mr. Tresh is requesting permission from ITA to create the ESWG as the state's formal cybersecurity technical working group and report to the ITA.

Chairman Weak opened the floor for discussion.

Ms. Robertson asked if non-state entities would be involved similarly to how the IGC-EC operates. Mr. Tresh replied it would not include non-state entities.

Ms. McArthur asked what the relation of the ESWG would be to ITLC. Mr. Tresh deferred to others on the structure of the ITA and its committees. Mr. Zickau clarified some pros and cons. The members of the ESWG are likely to be the people who work for members of the ITA and ITLC. The ESWG can report to either ITA or ITLC; the important thing is we have a formally recognized cybersecurity group. Historically, policies have gone before the subcommittees prior to being approved by the ITA primarily as a professional courtesy; there is no requirement for that process.

Ms. McArthur asked if the existing working group would remain in place or if this would replace that group. Mr. Zickau indicated this is an effort to formally acknowledge the existing group and there is no effort to displace the current members. Chairman Weak added there were three groups consisting of the same people that met about similar issues but there was nothing formalizing the groups. The intent is to formally consolidate those three groups and have them recognized by the ITA. It is also important to give cybersecurity the prominence it deserves as the citizens do not have a choice but to entrust the state with a huge amount of personal data. The state has a huge responsibility to safeguard that information.

Mr. Richard inquired about the existing processes for current IT policies and current work groups. Chairman Weak advised there were three security groups consisting of the same members who worked through all the cybersecurity policies currently in place. Those policies are generally vetted through the ITLC before going before the ITA. Mr. Tresh confirmed there was the Incident Response Task Force, the Critical Controls Working

Group, and the Cybersecurity Working Group, which accounted for about eight hours of meetings per month. It made more sense to consolidate the three together to address all issues under an Enterprise Security Working Group. This consolidation was discussed with the support of the ITLC chair.

Mr. Ben Call commented on the past direction from the ITA and asked if there has been any consideration for the defined responsibilities of the ESWG and if there would be any overlap with ITLC's responsibilities. Mr. Tresh advised the function of the group would not differ from the current process; the ESWG would still make recommendations to the ITLC on policies and related matters. They are looking to formally recognize the group and create formal processes.

Mr. Ross recalled a conversation with the former ITLC chair about their desire to create a technical working group over security and cybersecurity. Subsequent to that conversation, the topic was addressed at an ITLC meeting where the members gave a head nod agreement to its formation, which then broke into the three separate committees. As he recalls, the existing cybersecurity TWG was formed by ITLC. Chairman Weak asked if Mr. Ross recalled the timeframe of the TWG formation because this is where today's discussion stemmed from: there was nothing in the ITLC minutes that staff could find showing the formal creation of the group. Mr. Ross replied that there probably wouldn't have been anything in the minutes as this was an informal action taken by the committee.

Mr. Zickau proposed the ITA formally recognize the ESWG largely comprised of the individuals currently in the technical working group; their first order of business is to create a charter for ITA to review proposing roles and responsibilities; then the ITA can best determine what form it should take and where it should report.

MOTION: Mr. Zickau moved the ITA formally recognizes an Enterprise Cybersecurity Working Group to be chaired by the ITS CISO, Keith Tresh; their first order of business is to prepare a working charter for ITA to determine proper organization structure and other elements; Mr. Call seconded; the motion passed unanimously.

GEM UPDATE

Alberto Gonzalez, DMV Division Administrator, provided the committee an update on the GEM program. He explained all the services DMV provides and backstory for their modernization. Idaho Transportation Department (ITD) was dealing with a 40-year old legacy mainframe system where they needed to migrate data and eight distinct functions into one primary system and two freight systems. ITD decided to create the new system rather than hire a vendor because of the large failure rates other states were experiencing at the cost of millions of dollars to repair.

Mr. Gonzalez set the record straight about some misconceptions reported with the DMV system in 2018. At the beginning of their implementation timeline in 2016, they contracted with a vendor to replace the ten year old scanners, camera, and signature pads. That vendor began to have serious issues that shut down the systems across the state, which happened to coincide with the rollout of GEM in 2018, causing a lot of negative media attention. The developers from the GEM program were able to recreate the set up and get DMV back online within just a couple hours.

COVID-19 also caused significant delays to an already stressed system. DMV typically processes 10,000-12,000 transactions per day, but in October 2020, those averages went down to 7,000-10,000. It took DMV about two months to normalize production but they are still backlogged and many employees are not back to work yet. They are supplementing with temporary employees to help out.

The root cause of the October 2020 issue was data. They merged 40-year old data that had never been validated and staff spent thousands of hours cleaning and testing data in GEM. Before they went live, they did not realize how bad the data was and it caused significant delays. Since then, a lot of cleanup has occurred, nearly 800

system improvements have been implemented, and they are utilizing Access Idaho to process more online transactions than ever.

DMV has continued improvements scheduled over the next two years. They are working with counties and legislative ideas to continue improving customer service.

Chairman Weak thanked Mr. Gonzalez for the update and acknowledged the amount of work that went into this project.

ADOBE/MICROSOFT ENTERPRISE UPDATE

Chairman Weak moved the Adobe and Microsoft update to the next ITA meeting in the interest of time.

OTHER BUSINESS

Chairman Weak noted that budget requests for FY23 are coming up along with some additional federal funding coming to the state. As agencies are putting together their decision units, he reminded them about the IT Approval Process and ITS will be working with Division of Financial Management and Division of Purchasing to ensure requests have been vetted properly.

ADJOURNMENT

MOTION: Mr. Richard moved and Ms. Robertson seconded a motion to adjourn; the motion passed unanimously.

The meeting adjourned at 3:19 pm. The next meeting of the ITA will be scheduled at a later date.

Kristin Bartz, Office of IT Services