High Value Assets (HVA) Lessons Learned for Small Government Agencies and Small to Mid-sized Organizations

Natalie Sjelin
UTSA CIAS
Natalie.Sjelin@utsa.edu

Jeremy West
UTSA CIAS
Jeremy.West@utsa.edu

Glenn Dietrich Ph.D.
UTSA COB
Glenn.Dietrich@utsa.edu

Abstract

Cyberattacks are a persistent threat to organizations across all sectors, and over the past decade, attackers have increasingly been targeting municipalities. Protecting the most critical information and systems or high value assets (HVAs) from a cyberattack is essential to reduce the risk of impacting critical services that make day-to-day activities possible. Identifying HVAs is a process that assists organizations in recognizing which assets are most critical and therefore require the most significant protective measures. An HVA process was developed for State, Local, Tribe, and Territory (SLTT) jurisdictions of any size, capability, and cybersecurity maturity to assist them in identifying assets that are vital to community operations. The SLTT HVA Process aligns with the Federal HVA Program developed by the Cybersecurity and Infrastructure Security Agency (CISA). Four jurisdictions are piloting the SLTT HVA Process and, through this initiative, are generating vital lessons learned that will be used to successfully incorporate the process into their cybersecurity program.

Keywords: High Value Asset, HVA, critical assets, SLTT, lessons learned.

1. Introduction

Every organization is at risk of a network hack, data breach, malware, or ransomware attack, and for that reason, the protection of the organization's most important assets is critical. Every industry is at risk of a cyberattack, but over the past decade, local governments have increasingly become targets of cyberattacks. Emsisoft, a software firm, reported in 2019, 113 state and municipal governments and agencies were impacted by ransomware attacks resulting in disruptions that could put people's health, safety, and potentially lives at risk (Emsisoft Malware Lab, 2019). During the first two quarters of 2020, another 60 government entities were impacted by ransomware, including cities, transportation agencies, police departments, and one federal agency (Emsisoft Malware Lab, 2020). Research conducted by Barracuda Networks indicates that 44% of global ransomware attacks in 2020 targeted municipalities (Eytan, 2021).

Local governments are particularly attractive to cyber attackers as online government services expand, creating new attack vectors. Local governments often lack sufficient resources to protect and defend themselves against even the most basic attacks, not to mention sophisticated and persistent attacks (Forno, 2022). Attacks targeting local governments may be focused on financial gain. However, some malicious actors such as nation-states or cyberterrorists may be focused on disrupting society at the local level. "From issuing business licenses and building permits and collecting taxes to providing emergency services, clean water, and waste disposal, the services provided by local governments entail an intimate and ongoing daily relationship with citizens and businesses alike. Disrupting their operations disrupts the heart of U.S. society by shaking confidence in local government and potentially endangering citizens" (Forno, 2022). Additionally, the Nation's capability to manage risks associated with the increasing technological interconnectedness has historically outpaced capabilities to protect those technological advancements (Department of Homeland Security, n.d.).

Researchers at the University of Maryland, Baltimore County, have studied over 90,000 local governments' cybersecurity preparedness. As part of the research, local government chief security officers reported: "…that nearly one-third of U.S. local governments would be unable to tell if they were under attack in cyberspace" (Forno, 2022). The Multi-State Information Sharing and Analysis Center (MS-ISAC) conducts the Nationwide Cybersecurity Review (NCSR) annually to survey states, locals, tribes, and territories (SLTTs) about their organizational cybersecurity posture and top security concerns. Year after year, the chief security concerns include lack of funding, availability of cybersecurity professionals, and absence of a cybersecurity strategy (2019 Nationwide Cybersecurity Review, 2020).

URI: https://hdl.handle.net/10125/102843
978-0-9981331-6-4

In an effort to assist SLTTs in enhancing their cybersecurity posture, the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA), in cooperation with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has developed an SLTT High Value Asset (HVA) Pilot. An HVA process is vital for any cybersecurity program. Identifying high value assets assists decision-makers and stakeholders with prioritizing the most critical assets to secure and protect. Furthermore, implementing an HVA process into the fabric of an organization provides leaders with an objective mechanism for prioritizing financial resources against risks and threats. This paper will outline the SLTT HVA Pilot initiative and summarize lessons learned from implementing the process in four SLTT jurisdictions.

2. HVA Pilot Overview

The SLTT HVA Pilot is designed to align with the Federal HVA Program, established in 2015 through a directive from the Office of Management and Budgets (OMB). OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) directs the U.S. Federal Civilian Government to strengthen their cybersecurity through five objectives. One of these objectives requires agencies to identify, prioritize, and protect their high-value information and assets, resulting in the HVA Program (Office of Management and Budget, 2015).

OMB M-17-09 Management of Federal High Value Assets defines a seven-step process for federal agencies (*M-17-09 Management of Federal High Value Assets*, 2016). The seven steps in the federal HVA process are Plan, Identify, Categorize, Prioritize, Report, Assess, and Remediate. While these steps follow a logical order for an HVA process, there are some assumptions built into how and why these steps function in a federal environment. These include laws, regulations, rules, and systems across federal departments and agencies. In addition, the federal government has defined a list of primary mission essential functions by department, whereas some SLTTs have not (*Primary Mission Essential Functions by Department | Homeland Security*, 2015).

SLTTs vary widely in administration, economy, infrastructure, and population. Moreover, SLTTs range in size and type from the Puyallup Tribe of Indians with 4,000 members (Puyallup Tribe of Indians, 2016) to the State of California with a population of almost 40 million (*U.S. Census Bureau QuickFacts*, n.d.). Given the vast disparity between different SLTTs in size, resources, and capabilities, the CIAS designed the SLTT HVA Process to be flexible and scalable. This approach allows the process to be utilized by small to medium-sized SLTTs and will allow larger or more capable jurisdictions to enhance and mature their processes until they can easily leverage the Federal HVA process.

The design of the SLTT HVA Pilot is based on an evaluation of the SLTT landscape to include their overall cybersecurity maturity, capabilities, and resources such as personnel and budget. The design also considers the SLTT governance structure, recognizing that jurisdictions may be centralized, decentralized, or hybrid. Analysis and examination from reports, studies, articles, reviews, and interviews identified eight criteria that needed to be considered for the design and implementation of a successful SLTT HVA Program, including (Sjelin & Dietrich, 2022):

- a justification and benefits
- no or low-cost solutions
- suitability for information technology (IT) personnel with different capabilities
- flexible implementation timeframe
- tasks that need to be accomplished are more important than specific roles
- reuse existing organizational artifacts with HVA components
- provide a compelling value proposition for non-technical audiences
- uncomplicated processes, tools, templates, and checklists

The development of the SLTT HVA Process incorporates the above criteria providing a step-by-step approach. The approach enables all organizations or agencies, no matter their size, resources, or maturity in cybersecurity, to improve their efforts to identify and protect high value assets critical to the organization. The goals and outcomes of the CISA SLTT HVA project are to:

- improve SLTT High Value Asset Management
- leverage and adapt the federal process to SLTTs
- develop an SLTT HVA process (plan, identify, categorize, prioritize, report, assess, and remediate)
- develop supporting tools and guidance to assist implementation of the SLTT HVA guidance

The SLTT HVA Process is being assessed through an HVA Pilot where four jurisdictions will implement the process. The goals and outcomes for the pilot are to:

- test the validity of the guidance for understandability, identify gaps, and test the effectiveness and efficiency of the process
- test the validity and usability of the tools and worksheets

- determine or validate implementation timelines
- gather lessons learned

The recommended timeline to complete the SLTT HVA Process is 90 days. The timeline is flexible, understanding that the jurisdiction may be impacted by incidents and events that might prevent the pilot's completion within the 90-day period.

During the kickoff, a communication plan was established with each pilot jurisdiction. The plan included meetings after each phase milestone. Bi-weekly meetings continue to be held to discuss the project status and to address any problems or concerns as they arise. In addition to the planned communications, ad-hoc meetings are implemented on an "as needed" basis.

A website with the HVA toolbox was provided to each pilot jurisdiction to download the tools and documents needed to implement the SLTT HVA Process. The HVA toolbox contains:

- A description of the HVA Pilot Program
- Getting started
  - Identify High Value Assets guidance document
  - Quick start checklists
  - HVA Planning Workbook
- Identify and Prioritize
  - HVA Identification Questionnaire
  - Identify Mission Essential Functions (MEFs) guidance document
  - HVA Validation & Prioritization Tool
  - MEF and Asset Workbook
- Assess HVAs
  - HVA Assessment guidance document
  - HVA Self-Assessment Tool
- Remediation Action Plan
  - Action Plan template

Critical takeaways for jurisdictions participating in the HVA pilot include:

- An inventory of high value assets (HVAs)
- A listing of Mission Essential Functions
- A method to inventory and prioritize all organizational assets
- A process to assist risk-based decision making to invest time and resources based on identified critical assets and impact analysis
- A strategic action plan for implementation of security controls for HVAs

3. HVA Pilot Phases

The SLTT HVA Process defines five phases to manage the HVA lifecycle. The five phases are: Planning, Identify Mission Essential Functions (MEFs), Identify and Prioritize HVAs, Assess HVAs, and Develop a Remediation Action Plan. Each of the workbooks and tools used for these phases was developed in Microsoft Excel. Microsoft Excel was selected due to its near-universal availability across organizations and the ability to be quickly modified based on feedback from pilot participants.

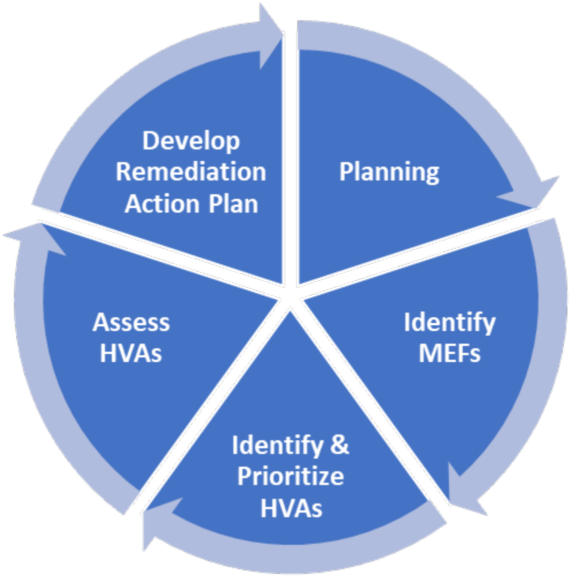

Figure 1. SLTT HVA Process

3.1 Planning

The planning phase helps guide leadership, stakeholders, and implementation teams through the HVA process. In this phase, SLTTs outline a stakeholder engagement plan, determine how the governance and oversight will work, and consider how HVA activities will be completed.

The planning phase can be managed using the HVA Planning Workbook. This tool contains a series of worksheets designed to aid in the capture of project-related information such as stakeholders, assumptions, and schedules. Steps in this phase utilize the HVA Planning Workbook and include:

- Define HVA process
- Document requirements
- Identify key stakeholders
- Establish the HVA process team
- Identify HVA components
- Creation of the schedule
- Kickoff the project

Each phase contains a minimum viable outcome. A minimum viable outcome is the essential deliverable need from the phase to proceed to future phases. In some cases, all potential or possible deliverables from a phase may not be necessary to move to a future phase. The minimum viable outcome of the planning phase is a list of stakeholders and organizational units.

3.2 Identify MEFs

In this phase, SLTTs identify mission essential functions (MEFs). Organizations may have identified some or all their MEFs as a part of another emergency, continuity, disaster, or asset management effort. This phase utilizes a MEF and Asset Workbook. The MEF and Asset Workbook allow participants to capture and document information acquired from the following steps:

- Creation or updating of the SLTT MEFs (Organizational MEFs)
- Mapping organizational units to SLTT MEFs
- Creation and association of unit MEFs to SLTT MEFs
- Identification of critical assets and data required to support the unit MEFs

The minimum viable outcomes in this phase include a list of organizational unit MEFs, IT assets tied to each unit MEF, and a list of critical assets, which are candidate HVAs for the next phase.

3.3 Identify and Prioritize HVAs

The Identify and Prioritize HVAs phase is foundational to obtaining a hierarchical list of the organization's most essential assets using objective criteria. This step allows SLTTs to review proposed HVAs, and validate and prioritize them according to the organization's mission and what is deemed critical. This phase leverages a Validation and Prioritization Tool to determine if a critical asset is an HVA. The Validation and Prioritization Tool contains several worksheets. First, an HVA questionnaire containing a series of questions participants answer about the critical asset. If the answer is yes to any of the questions, then the asset is classified as a candidate HVA. Candidate HVAs are entered into a worksheet in the Validation and Prioritization Tool. This worksheet enables the collection and documentation of essential information for each asset that is entered.

The types of information collected about each HVA include but are not limited to supporting a MEF, system interdependencies, Recovery Time Objectives (RTO), processing or storage of sensitive or protected data, modernization efforts, number of major incidents associated with the asset, number of network end-points, and the existence of one or more remediation activities for the asset. The minimum viable outcome for this phase is a list of prioritized SLTT HVAs. Prioritization is set by weights assigned to the questions in the HVA worksheet.

3.4 Assess HVAs

The HVA assessment phase aims to identify vulnerabilities and predisposing conditions in the HVA security environment that increase the risk to the organization or the SLTT. The HVA assessment is based on the prioritization of the HVAs, and the organization's risk tolerance. The assessment derives from the National Institute of Standards (NIST) Cybersecurity Framework (CSF) version 1.1. The CSF was selected for several reasons, but primarily due to the widespread usage by SLTTs as a part of the annual NCSR. The HVA CSF Self-Assessment Tool is used in this phase. The tool contains a series of spreadsheets containing the CSF controls, status dashboards, and reports detailing the current state of the HVA assessment.

During the assessment phase, organizations select a range of HVAs to assess based on their priority, such as a top-five or top-ten and enter them in the HVA CSF Self-Assessment Tool. After the in-scope HVAs are added to the tool, the assessor(s) evaluate them against 108 outcome-driven statements, or subcategories, across the CSF's Identify, Protect, Detect, Respond, and Recover core functions. The assessment is based on two areas: a defined policy and control implementation. The defined policy pertains to the state of the organization's policy related to the specific outcome. Here, an evaluator determines the state of the organization's policy, such as whether it is informal or formal, written and approved, or doesn't exist. The second area is the implementation level which refers to how well the organization has accomplished the specific control or outcome. The evaluator assesses if the controls are implemented at the HVA or organization levels. Not all controls have to be assessed on a per HVA basis as some controls are organizationally based.

The evaluator continues to assess the organization's implementation of the controls through each CSF core function until all the outcome-driven statements have been assessed. Once the assessment is complete, organizations will automatically generate a report of the evaluation based on a moment in time. The report generation step is vital because the CSF Self-Assessment Tool is dynamic, and any changes will automatically change dashboards. The outcome of this phase is a list of CSF gaps both at the policy and implementation levels.

3.5 Remediation Action Plan

In the Remediation Action Plan phase, organizations craft plans to address the gaps identified in the HVA assessment phase. During this phase, organizations use the HVA CSF Self-Assessment Tool to remediate findings using documented risk response strategies and organizational priorities, resources, and risk tolerance. Risk response strategies are those actions taken by organizations to reduce risk to HVAs and ensure the continued sustainment of the organization's MEFs. Organizations can respond to risk in various ways, including risk acceptance, risk avoidance, risk mitigation, risk-sharing, and transfer of risk or a combination of two or more strategies. The steps in the Remediation Action Plan phase include:

- adding the gaps identified in the assessment phase to the remediation section of the HVA CSF Self-Assessment tool
- documenting the organization's response for each gap identified through the assessment
- submitting the remediation action plan for leadership approval
- implementing an approved remediation action plan
- assessing the effectiveness of the remediation action plan

The minimum viable outcome for the remediation action phase is a documented and approved way ahead to protect the organization and its HVAs.

4. CSF Profiles

In developing the Assess HVAs and Remediation Action Plan phases, it was evident that organizations needed a mechanism to limit the scope of activities while prioritizing assessment and remediation efforts. Framework Profiles became the ideal solution for scoping and prioritization efforts because profiles represent outcomes based on the business needs of the organization characterized by the Framework Core (Ibrahim et al., 2018).

A profile is a baseline recommendation describing best practices to secure a target system, asset, or organization. A profile enables organizations to establish a roadmap for reducing cybersecurity risk aligned with organizational goals. Given the complexity of many organizations, they may choose to have multiple profiles aligned with particular components (such as HVAs) that recognize their individual needs. Framework profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The current profile indicates the "as is" organizational cybersecurity state, and the target profile indicates the "to be" state or based on cybersecurity risk management goals (National Institute of Standards and Technology, 2018).

Profiles support mission requirements within the organization and aid in communicating risk between organizations. Creating a profile is vital for communicating current risk, target-risk, and cyber resilience with all parties involved in an HVA project. Better communication is essential to making progress in every cybersecurity program. The HVA CSF Self-Assessment Tool comes with two preloaded profiles, although organizations are free to choose their own. The preloaded profiles are 1) SLTT HVA Profile and 2) Cybersecurity Framework Profile for Ransomware.

4.1 SLTT HVA Profile

The CIAS created this profile at UTSA to help SLTTs of various sizes identify and prioritize those controls or outcomes that are fundamentally important based on other guidance. The profile is derived from three sources listed below:

- Cyber Essentials Starter Kit– this guide, created by CISA, is for leaders of small businesses and local government organizations. It is designed to help develop an actionable understanding of where to begin implementing organizational cybersecurity practices (*Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness*, 2021). It is consistent with the NIST Cybersecurity Framework and is a starting point for cyber readiness. The Cyber Essentials Starter Kit, published in Spring 2021, outlines the things to do first, including Backup Data, Multi-Factor Authentication, and Patch and Update Management.
- Securing High Value Assets – this document was published by DHS in July 2018 (Kelly, 2018). It presents six findings from previous HVA Agency Assessments conducted by DHS. Each finding provides examples of issues and challenges in implementing and maintaining robust security capabilities to protect HVAs. In addition, each finding maps to the corresponding CSF core functions to provide security outcomes and activities.
- Cybersecurity Maturity Model Certification (CMMC) version 1.0 Level – The Department of Defense's Cybersecurity Maturity Model Certification is designed to assess and enhance the cybersecurity posture of the Defense

Industrial Base sector, including all contractors. CMMC Level 1 is achievable for smaller organizations and includes a subset of universally accepted standard security practices (Cybersecurity Maturity Model Certification, 2020). The mapping for this part of the SLTT Profile was performed by cross-referencing NIST 800-53 v5 controls between the CMMC and CSF.

4.2 Cybersecurity Framework Profile for Ransomware Risk Management

NIST created the Ransomware profiles to identify those security objectives that aid with prevention, response, recovery, and management of a ransomware incident. The profile can be used as a guide to manage the risk of ransomware events" and "includes helping to gauge an organization's level of readiness to counter ransomware threats and to deal with the potential consequences of events (Barker et al., 2021)."

Organizations may build or select one or more profiles based on the organization's desired cybersecurity outcomes to provide flexibility and scalability. In addition, organizations may add their own Categories and Subcategories based on unique risks, requirements, and priorities.

5. HVA Pilot Participants

The HVA Pilot participants are made up of various sized jurisdictions. Participants represent one state, one municipality, and two counties or parishes. At the onset, the goal is to have different types of jurisdictions of various sizes perform the activities outlined in the SLTT HVA Process. While performing the activities, the objective is to assess the overall process and evaluate the developed guidance, tools, and templates. Specifically, pilot participants will provide feedback on the implementation complexity, processes, guidance, and tools. Pilot participants were selected based on existing contacts, recommendations, a willingness to commit time and resources, and leadership buy-in.

The HVA Pilot participants started the process at different times. Participant #1 began the process in July 2021. Participant #2 began the process in February 2022 and Participants #3 and #4 started the process together in May 2022. Participant #1 has completed the process having gone through all phases of the SLTT HVA Process. Participants 2, 3, and 4 are at various stages in the SLTT HVA Process.

The pilot participants are described by four primary characteristics, including entity type, population, size of IT organization, and HVA pilot participation. The population statistics for the jurisdictions are rounded to the nearest hundred thousand and were obtained from the US Census Bureau's QuickFacts website (*US Census Bureau QuickFacts*, n.d.). IT organization size and organizational pilot participation are estimates obtained through a survey completed by the pilot participants.

5.1 Pilot Participant #1

Type: Municipality
Population: 200,000
IT organization size:

- Dollars: $7.2M
- IT personnel: 43
- Cybersecurity personnel: 6

Pilot Characteristics:

- Dedicated resources: 2
- Total organizational units: 42
- Organizational units in the pilot: 14

5.2 Pilot Participant #2

Type: State (Agency)
Population: 1,500,000
IT organization size:

- Dollars: $30M
- IT personnel: 200
- Cybersecurity personnel: 8

Pilot Characteristics:

- Dedicated resources: 7
- Total organizational units: 9
- Organizational units in the pilot: 3

5.3 Pilot Participant #3

Type: County/Parish
Population: 400,000
IT organization size:

- Dollars: $8.6M
- IT personnel: 36
- Cybersecurity personnel: 3

Pilot Characteristics:

- Dedicated resources: 3
- Total organizational units: 45
- Organizational units in the pilot: 40

5.4 Pilot Participant #4

Type: County/Parish
Population: 100,000
IT organization size:

- Dollars: $ 1.5M
- IT personnel: 10

- Cybersecurity personnel: 0

Pilot Characteristics:

- Dedicated resources: 2
- Total organizational units: 20
- Organizational units in the pilot: 20

6. Lessons Learned

The HVA Pilot is currently ongoing, and lessons learned continue to be gathered. One pilot organization has completed the SLTT HVA Pilot. The estimated completion of all pilots is September 2022; however, additional time has been allotted to allow for unforeseen events that may impact the jurisdictions' implementation timeline. The lessons learned captured to date are based on the discussions with the pilot participants during status and milestone meetings as they go through the process. Significant lessons learned are disclosed in this section and presented by topic.

6.1 Simplifying MEF Process

As feedback from the first pilot emerged, it became clear that some HVA processes needed additional implementation steps. Evidence from Pilot #1 demonstrated that identifying MEFs needed to be a separate phase instead of a step in the Identify and Prioritize phase. This was due partly to its importance in mapping HVAs to the jurisdiction's MEFs and identifying the corresponding organizational units supporting that MEF. In addition, the federal government has identified their MEFs and mapped them to the appropriate agencies; however, many SLTTs have not performed this step, and it often is beyond the scope of a single department.

Additional feedback from Pilot #1 revealed that the initial MEF processes, leveraged from FEMA guidance and templates, were cumbersome and challenging to navigate and execute. To rectify these issues, the MEF guidance was reviewed and consolidated into just those essential steps needed to identify mission essential functions and link critical assets to those MEFs by organizational units. This phase was further simplified by the creation of the MEF and Asset Workbook. The workbook not only included suggestions from Pilot #1 but also enabled the consolidation of all the pertinent tables, templates, and tools into one location.

6.2 Data Confidentiality and Integrity

Pilot participants easily identify the impacts of information and systems when they are not available to employees and customers. They do not consistently consider the confidentiality and integrity impacts. Participants benefit from reminders to consider confidentiality and integrity when identifying candidate HVAs. One example, provided by a pilot participant, described how important this concept is especially where the information is used by law enforcement. In cases where information is retrieved and used in a legal case, there cannot be any indication that the value of the information is in question. If there is a concern that the information has been changed or modified in any way, all cases will then need to be reevaluated because the credibility of the information is in question and this will introduce reasonable doubt in a court case resulting in an automatic not guilty verdict.

There is a tendency in continuity planning, disaster recovery, and asset management to leverage RTO to order recovery and protection priorities. However, this fails to capture the sensitivity, importance, privacy, and integrity of the data. The genesis of the federal HVA program was due to two data breaches involving millions of extremely sensitive records from U.S. Office of Personnel Management (OPM) (Baan, 2018). The system contained sensitive data about millions of Americans.

In 2019, the City of Baltimore experienced a ransomware attack against the city's information and systems. The financial impact was at least 18.2 million dollars, which included a potential 8.2-million-dollar loss due to "delayed revenue, such as money from property taxes, real estate fees, and some fines (Duncan, 2019)." These examples illustrate the importance of data confidentiality and integrity when identifying HVAs. As a result, when evaluating assets for HVAs, organizations should consider the sensitivity or importance of the data in their environment.

6.3 Expanded Benefits

As the pilot participants work through the process, additional benefits continue to be identified. Initially the key takeaways, as previously described, include an inventory of HVAs; list of MEFs; a method to inventory and prioritize organizational assets; a process to determine where to apply time and resources; and a strategic plan for implementing additional security for HVAs. The pilot participants continually identify more benefits than originally considered. These expanded benefits are described as follows:

- **Building relationships throughout the jurisdiction**. As the pilot participants work with departments and agencies throughout the community, they have indicated that they are enhancing established relationships with those entities and, in some cases building new relationships. Implementing the HVA process with inputs from as many stakeholders as possible brings the community closer together. The result is the alignment of interests, such as the protection of mission essential functions across the jurisdiction.

- **Establishing or enhancing asset inventories**. Not all of the pilot participants have an established asset inventory. As participants work through the pilot, they can leverage the HVA process to establish an asset inventory. In addition, other pilot participants have disclosed that the HVA pilot program allows them to validate or enhance existing asset inventory initiatives. Furthermore, the HVA process enables participants to identify and prioritize assets in their inventory.
- **Incident Response Efforts.** During the pilot, the Log4j zero-day vulnerability occurred and the jurisdictions conducted incident response efforts to scan for the vulnerability. One of the pilot participants commented that if they had completed the HVA pilot, the inventory of HVAs would have been beneficial in identifying critical assets to respond to first.
- **Aligns with Other IT efforts.** Other IT efforts such as IT modernization and continuity planning efforts are aligning with the HVA pilot. Assets identified through this project can be used to assist with decision-making and to ensure other efforts have complete asset information.

6.4 Guidance and Tool Simplification

Guidance needs to be simplified and tools need to be intuitive. Some of the participants have not had the time to read through the guidance completely or have tried to use the tools without reading through the guidance. As a result, SLTT HVA Processes and tools were misunderstood. To provide more simplified guidance, the use of the checklists was reinforced and videos were created to provide a quick overview of how a tool should be used and what information should be gathered. All templates were turned into workbooks to gather information. This became a very intuitive process allowing the participants to quickly identify what information was needed.

6.5 Implementation Timeline

The timeline flexibility is a necessary consideration and validation of this has been recognized. In addition to the flexibility, dedication from the participants is necessary to implement the process. During the first pilot, three major disruptions impacted the HVA implementation timeline. In the first instance, the participant was tasked with additional duties to support the distribution of COVID vaccines. This entailed supporting communications and systems to track the distributions. In the second instance, a major weather-related issue disrupted normal operations and support of ensuring the jurisdiction was back up and running was necessary. The third instance was to respond to the Log4j zero-day vulnerability. In this case, identifying scanning methods that would successfully identify which assets were susceptible to the vulnerability and then scanning all assets took significant time. In addition to these major incidents, the expected downtime for illness of staff and leave time also transpired.

6.6 Stakeholder Involvement

Stakeholders involved in the SLTT HVA Process added some obstacles for the pilot participants. In some cases, stakeholder participation was completely voluntary as the governance structure was of a decentralized or hybrid nature. This scenario required additional stakeholder engagements to explain the benefits and overall process. Additionally, working with stakeholders to identify MEFs and candidate HVAs also took extra time. In some cases one-on-one meetings produced a consensus on the organization's MEFs or identification of critical assets. One last observation, thus far, includes taking into consideration stakeholder workloads. In one case, a stakeholder was unable to complete the process with the pilot participant due to an increased workload that took priority. In this particular case, the stakeholder was law enforcement and they experienced an increase in crime which shifted their priorities during the pilot resulting in the agency being unable to continue the project.

6.7 Policy Development

Not all pilot participants have security policies, or at least they may be at various implementation stages. For example, the specific security policy component may be informal, documented but not signed, and so forth. As participants use the HVA CSF Self-Assessment Tool, they can identify policy gaps and leverage the tool to track the policy stage and status.

7. Results

While the results of the pilots will be ongoing, some outcomes such as the development of asset inventories, stakeholder participation, and overall value are worth mentioning. One of the first results identified by pilot participants was recognizing that the pilot functioned as the first step in building an asset inventory. Some organizations struggle with the scale and scope of beginning asset management efforts, but the SLTT HVA Process helped participants initiate asset management efforts focusing on the most critical assets first.

SLTT HVA Pilot participants experienced varying levels of participation from organizational units. Participation was limited for several reasons, including a desire by pilot participants to limit the scope of the HVA activities, the willingness of organizational units to participate in HVA efforts, and separate authority structures. Despite these results, pilot participants have and continue to achieve positive results. Furthermore, several participants plan to expand HVA processes to additional units as a part of a periodic review and expansion of HVA efforts.

A vital pilot objective is to receive feedback, not only on the components of the pilot but on the overall value of the HVA initiatives undertaken by participants. In addition, preserving the anonymity of pilot jurisdictions and participants is an essential trust-building activity. As such, participants are referred to using the role they hold instead of their name. One pilot participant offered the following regarding the value of the HVA pilot for their organization:

"While we have always and especially recently prioritized cybersecurity, we have struggled with the sheer volume of assets we must protect - including knowing the locations of these assets and which ones we need to prioritize to maintain critical operations. This program has helped us identify and prioritize those assets for maximum protection, redundancy, and disaster response investments, supported by systems and processes that will help mitigate the effects of any cyber-attack or intrusion (Pilot Participant Director of Information Systems, personal communication, February 3, 2022)."

8. Conclusion

There are four jurisdictions participating in the SLTT HVA Pilot designed specifically for the SLTT community. The SLTT HVA Process provides security and IT leaders with essential information to objectively justify measured responses to security challenges or gaps within their organization. The program ties the most critical systems and data to MEFs while prioritizing the HVAs based on objective criteria and the most significant risks. The objective criteria are gathered across HVAs, prioritized, and assessed against standards, guidelines, and best practices to manage cybersecurity risks.

SLTT HVA efforts synthesize cybersecurity risks into digestible and discrete organizational or business priorities, ensuring that new expenditures maximize the protective return on investment. Using HVAs to prioritize investments ensures each dollar protects the most critical assets based on threats and vulnerabilities to the organization's mission. In addition, instituting a formal HVA process as a component of an organization's cybersecurity program can serve as the precursor for building an asset management capability. Several SLTTs do not have an asset management process; if they do, it may be incomplete. As a result, HVAs are becoming a priority in the asset management process for protection and modernization initiatives.

Furthermore, incorporating HVAs as a part of an asset management program enables organizations to respond to emerging critical vulnerabilities such as Log4j. During the pilots, CISA issued guidance encouraging organizations to identify and remediate vulnerable Log4j instances based on the scope of covered assets (*Apache Log4j Vulnerability Guidance | CISA*, 2022). Pilot participants lamented not having completed the SLTT HVA Process earlier because they believed it would have allowed them to better identify and prioritize remediation efforts.

This research highlights the genesis of and essential characteristics of an SLTT HVA Pilot. Pilot participants include a state agency, county or parish, and municipality. Participants leverage a five-phase approach outlined in the SLTT HVA Process. These processes include planning, identification of MEFs, prioritization of HVA, assessment, and remediation. In addition, some valuable feedback has already led to simplification and improvements in overall processes. Furthermore, results from the pilot demonstrated the intrinsic and ancillary benefits of incorporating an HVA process into cybersecurity programs. Lastly, additional research with smaller jurisdictions, tribes, and territories using the existing or an alternative assessment framework could lead to significant improvements in the SLTT HVA Process.

9. Next Steps

The next steps for SLTT HVA initiative include updates at the programmatic level and broadening the audience.

Development of training programs targeting audiences involved in the SLTT HVA Process would significantly enhance the execution of future HVA initiatives. The result would significantly enhance the successful execution of HVA initiatives.

Incorporating the SLTT HVA Process with standards, guidelines, and best practices for continuity planning, disaster recovery, and incident management would allow organizations to focus these initiatives on critical assets.

Future research should involve jurisdictions of a smaller size than those who piloted this process. Determining how well the approach scales down to organizations with fewer resources and serving a smaller population is worthwhile. In addition, having communities much larger than those piloted in this initiative would be beneficial to assess the scalability of this approach.

10. References

2019 Nationwide Cybersecurity Review. (2020). Multi-State Information Sharing & Analysis.

Apache Log4j Vulnerability Guidance | CISA. (2022, April 8). Cybersecurity and Infrastructure Security Agency (CISA. https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Baan, A. (2018, July 18). *First Things First: Know Your Data | ISACA Blog*. ISACA Now Blog. https://www.isaca.org/en/resources/news-and-trends/isaca-now-blog/2018/first-things-first-know-your-data

Barker, W., Scarfone, K., Fisher, W., & Souppaya, M. (2021). Cybersecurity Framework Profile for Ransomware Risk Management (Preliminary Draft) (NIST Internal or Interagency Report (NISTIR) 8374 (Draft)). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/nistir/8374/draft

Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness. (2021). CISA. https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

Cybersecurity Maturity Model Certification (CMMC). (2020, January 20). https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

Department of Homeland Security. (n.d.). *National Preparedness Report* (December 2021).

Duncan, I. (2019, May 29). Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts. Baltimore Sun. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

Eytan, O., Dr. (2021, June 22). *Municipal cyberattacks: A new threat or persistent risk?* Forbes.Retrieved June 6, 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/06/22/municipal-cyberattacks-a-new-threat-or-persistent-risk/?sh=1938be303ffb

Emsisoft Malware Lab. (2019, December 12). State of Ransomware in the US: Report and Statistics 2019. Emsisoft. Retrieved June 8, 2022, from https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

Emsisoft Malware Lab. (2020, July 8). *State of Ransomware in the US: Report and Statistics for Q1 and Q2 2020*. Emsisoft. Retrieved June 8, 2022, from https://blog.emsisoft.com/en/36534/state-of-ransomware-in-the-us-report-and-statistics-for-q1-and-q2-2020/

Forno, R. (2022, March 29). *Local Governments Are Attractive Targets for Hackers and Are Ill-Prepared*. GOVERNING The future of states and localities. Retrieved June 12, 2022, from https://www.governing.com/now/local-governments-are-attractive-targets-for-hackers-and-are-ill-prepared

Kelly, R. E. (2018, July). Securing High Value Assets. https://www.cisa.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. The Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

M-17-09 Management of Federal High Value Assets. (2016). Office of Management and Budget. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Office of Management and Budget, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government", available from https://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-16-04.pdf, October 30, 2015.

Pilot Participant Director of Information Systems. (2022, February 3). Value of the HVA Pilot [Email].

Primary Mission Essential Functions (PMEFs) by Department | Homeland Security. (2015). https://www.dhs.gov/sites/default/files/publications/list_of_validated_pmefs_by_department_v2_fema.pdf

Puyallup Tribe of Indians. (2016). Climate Change Impact Assessment and Adaptation Options. Cascadia Consulting Group. http://www.puyallup-tribe.com/tempFiles/PuyallupClimateChangeImpactAssessment_2016_FINAL_pages.pdf

Sjelin, N., & Dietrich, G. (2022). Method to Identify High Value Assets for Small Government Agencies and Small to Mid-sized Organizations. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2022.283

Stone, B. (2022, March 4). Cyberattacks on SMBs are increasing. Will your business be ready? https://www.techrepublic.com/article/cyberattacks-on-smbs-are-increasing-will-your-business-be-ready/

US Census Bureau. (2022, May 26). Fastest-Growing Cities Are Still in the West and South. Census.Gov. https://www.census.gov/newsroom/press-releases/2022/fastest-growing-cities-population-estimates.html

U.S. Census Bureau QuickFacts: United States. (n.d.). US Census Bureau. Retrieved June 10, 2022, from https://www.census.gov/quickfacts/fact/table/US/PST045221