Managing Information Security System Technology Changes across an Enterprise

Kevin E. Foltz and William R. Simpson
Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, VA 22311

ABSTRACT

The goal of information security systems in an enterprise is to make the right information available to the right entities at the right times and in the right formats while ensuring only authorized information flows occur. The standard approach is to purchase a new system to meet current needs. Patches, work-arounds, and added components satisfy the changing future needs while creating an increasingly complex system, and operational capability slowly degrades over time as complexity builds. The system is then rebuilt from the ground up, at great cost and inconvenience, and the cycle repeats. This paper describes an approach for constant change. Instead of building the best system possible based on today's needs, only to replace it in the future, the goal is a system that is capable of evolving toward a better future in a consistent and directed way. This prevents one-off fixes from lingering, and it keeps the distributed decision-making process aligned toward a common enterprise goal. Components not consistent with future goals are identified and scheduled for replacement. Current practices chosen for expedience are assigned expiration dates to prevent them from becoming solidified in the future architecture. The replacement cycle is applied to components of the system instead of the entire system. This stops the cycle of complete replacements by allowing constant change, which reduces overall cost and maintains a more consistent operational capability.

Keywords: Enterprise, Implementation Baseline, Information Security, Operational Baseline, Target Baseline, Technology.

1. INTRODUCTION

Information security systems are complex. They are built using products with configurations, settings, and best practices that can be difficult to understand and implement. The products use protocols, which are instantiated in implementations that themselves have engineering trade-offs and configurations. These implementations build on underlying networking infrastructure, protocols, and configurations, and these rely on algorithms, mathematics, and physics to work. Just the simple act of loading a web page has built into it a vast array of technologies, configurations, settings, and other considerations developed over many years by thousands of individuals, companies, and other entities and refined by billions of users and trillions of interactions. This situation is only becoming more complex as new protocols, scientific research, products, and operational guidance are developed.

The first challenge for an enterprise is not just how to build a secure information-sharing system, but how to even define the goals in such a changing landscape. The goals must be set at the appropriate level. Too high, and they fail to guide real-world choices. Too low, and they become too rigid when new technologies emerge. With the right goals, the second challenge is to understand the past, present, and future. The past is all the systems already purchased and operating. The present is the set of systems being put into place now. The future is the vision for upcoming systems, and the direction in which to move current systems. With this understanding of past, present, and future, the final challenge is to integrate and manage these in a cohesive way. As time progresses, the future becomes the present, the present becomes the past, and the past is retired. This cycle should be continuous in order to preserve a functioning system rather than thrash between new and shiny systems with great promise that quickly become frustrating old systems that no longer function.

2. CURRENT APPROACHES

Some current approaches to information security system management rely on the expert, the bureaucracy, or the vendor.

The Expert

With the expert approach, a single expert or small group owns the problem and the solution to all information system issues. They plan, coordinate, and direct computer-related activities in an organization; help determine the information technology goals of an organization; and are responsible for implementing computer systems to meet those goals. [1] Their competence enables the enterprise to rely on them for all its needs, and the expert is rarely questioned. This is partly because their competence allows them to make good choices, keep systems running, and respond quickly to requests, but also because no one else in the enterprise is qualified to ask the right questions to challenge them. This approach has the benefits of efficiency, consistency, and good alignment with enterprise goals. However, if the expert is a single person or a small group, this person may have their own hidden agenda or biases that drive their decisions. This would be difficult to stop or even discover. Also, an individual or small group may retire, take another job, or otherwise leave the enterprise scrambling for a replacement. Because the system was maintained by a single person, it may have idiosyncrasies that this person created and kept up with, but others coming into the job would not understand. Thus, changing experts requires a complete system overhaul, where a lot of the accumulated knowledge about the system, its users, and best practices is lost. Relying on these experts can be beneficial in the short term, but they may limit the growth and continuous improvement of the organization. [2]

The Bureaucracy

A bureaucracy can address some of the failings of the expert. It is a system for controlling or managing an organization that is operated by a large number of officials employed to follow rules carefully. [3] Instead of a single person who is largely

unaccountable, a bureaucracy documents all of its procedures, processes, and decisions in detail. It often has oversight and periodic reviews as well. This allows the function of the bureaucracy to continue even as the people within it are constantly changing. However, bureaucracies often take a life of their own that can diverge from their original intent due to the tendency of the bureaucracy to try to survive through funding variances and changing political pressures. Also, bureaucracies are inefficient and slow to change, and they often make decisions based on who complains loudest or who has the most influence instead of who has the best ideas. They lack the accountability of a single person. [4] Where the expert can exercise good judgement on a case-by-case basis, bureaucracies are constrained by their own operating procedures, which do not always fit well with future problems that arise.

The Vendor

Vendors ultimately provide the products that are used to build information-sharing systems. They are current with technology, products, and best-practices. They anticipate future needs and work to meet them in their products. As a result, vendors often have better knowledge than a bureaucracy about how to build a system. Also, many vendors work as integrators to provide cohesive solutions for a related set of information-sharing problems. It is often tempting to go to vendors looking for solutions. However, the vendor goal is profit. Profit can be aligned with providing a good solution, but often in the long term it is not. In particular, vendors often strive to lock customers into their solutions by providing functionality that works well as part of their overall solution but does not integrate with other solutions. [5] When an organization is locked in, the vendor can increase prices until they are close to the significant cost to switch vendors. Comparing vendors or choosing a different vendor is not the solution, because the problem is inherent in the vendors' goals and the structure of the relationship.

3. THE VISION

A new approach is needed to address current problems. Our vision includes the following components:

- Describe design principles and goals
- Document the past, present, and future
- Trickle down from future to present to past
- Dedicate teams to continuously review and update documentation

The first part, where design principles and goals are described, forms the foundation for all later work. Current work on the Enterprise Level Security (ELS) security model starts with a set of tenets, a subset of which are shown in Figure 1. These are basic design principles that are used to build the ELS architecture.

Examples include simplicity, assuming malicious entities cannot be kept out of our system, extensibility, and accountability. These basic ideas and goals shape all detailed decisions for the system. Tied to these tenets are a set of key concepts for our system. These include important protocol decisions, the need to name all entities, and the need to authenticate all entities. Unlike the tenets, which could be applied to many different types of systems, the key concepts are related specifically to our information system. Tied to these concepts are a list of requirements. These include specific naming requirements, the requirement for unique identities, and the restriction against anonymity in communications. The requirements are still not particular to any product or service, but they apply generally across many products. These are high-level requirements for the entire information-sharing system. This basic security model, including the full sets of tenets, concepts, and requirements, is described in more detail in [6].

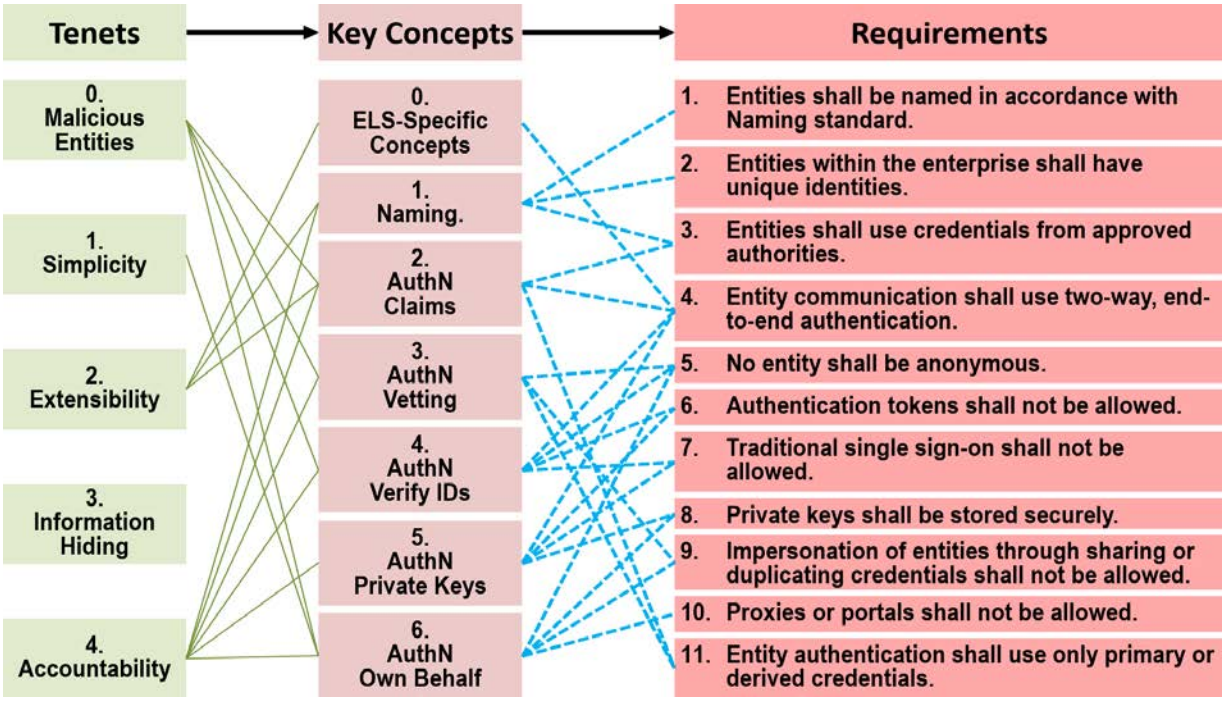

Figure 1 Mapping of Tenets to Concepts to Requirements

Beyond these tenets, principles, and goals are a set of documents that discuss specific technologies. These document the past, present, and future. The future is closely tied to the design principles and goals. This is the "Target Baseline," which consists of documents that describe the goal for the near future for different technologies. The first set of these documents consists of "Scenarios," which describe different enterprise needs and the questions they raise about how to use technology. The second part consists of "Technical Profiles," which describe how to use different technologies. These include authentication, access control, and other basic security functions. They also include mobile device management, databases, and operating systems, which rely on the basic security documentation and requirements. Scenarios are written as enterprise needs are identified. Technology profiles are written as the scenarios raise technology questions.

The scenarios and technology profiles describe the goal for the ideal future state. This is not constrained by current products or best practices. It seeks to apply the design principles and goals to particular technology problems by proposing technical solutions that are consistent with the design goals.

The present-looking documents are the "Implementation Baseline," which describe current products. Each document provides an assessment of how a currently available product compares against relevant Technical Profile requirements. "Capability Profile" documents bridge the gap between the Target Baseline and Implementation Baseline. These describe the capability a product implements and the relevant target baseline document requirements that apply.

A product with an Implementation Baseline document is not an approved product. It is simply a product that has been analyzed with respect to the goals for the security model and information sharing. With this analysis, it is possible to make informed decisions for risk management. The document identifies shortcomings in security and capability. It quantifies the security risks and provides forms of mitigation that may reduce risk.

The Implementation Baseline documents also include information about product vendor plans for the future, such as whether or when they plan to release an updated version that meets certain requirements or mitigates risks. For example, when setting up an encrypted communication path, a product may use several standard approaches. For many reasons, including vulnerabilities and compromises, the more current standards may be required as part of the baseline. The current release of a product may have implemented Transport Layer Security (TLS) version 1.0. This may not meet the baseline requirement of TLS 1.2 or subsequent. However, the developer may plan to provide TLS 1.2 in its next release. This future-looking assessment can be used to decide whether a product is more or less likely to meet future enterprise needs by comparing their plans to the future goals as stated in the Target Baseline. In some cases, the product will not be recommended if it is not on a path to satisfy the baseline.

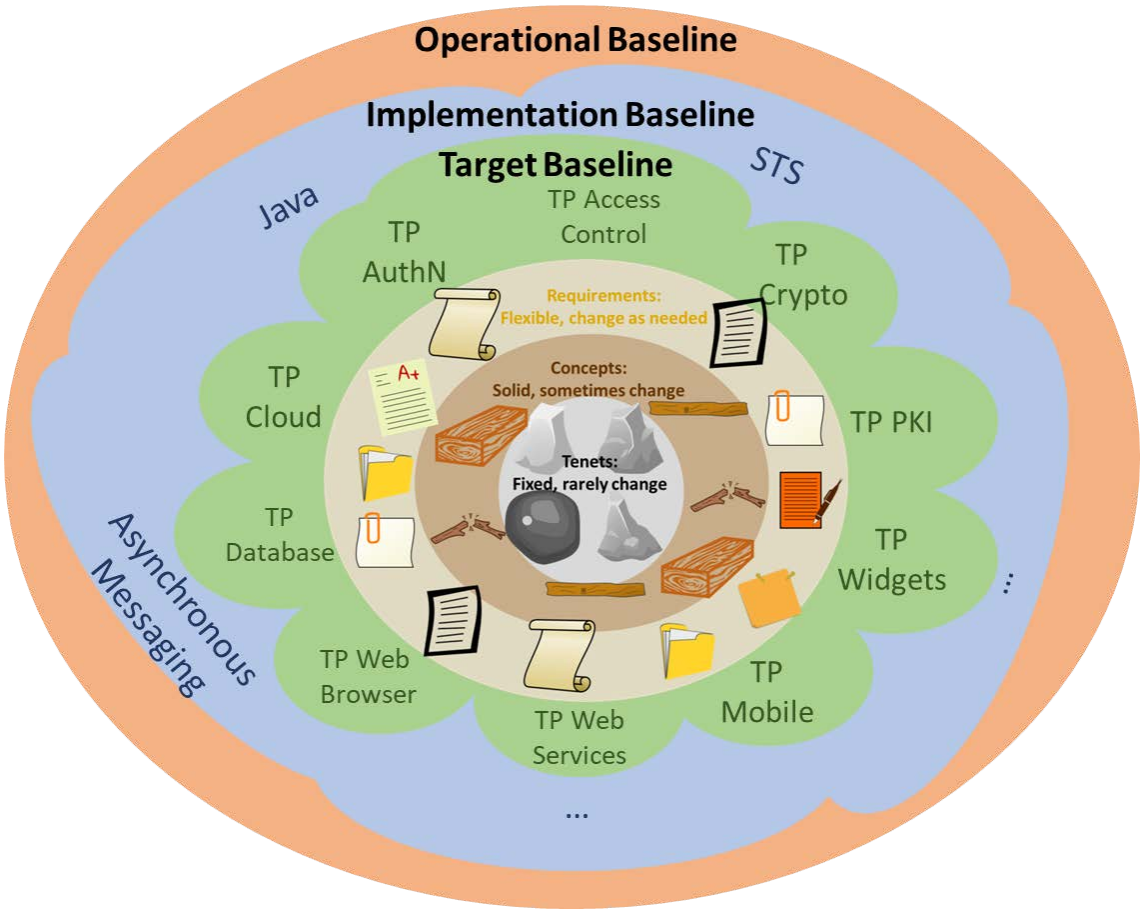

Figure 2 The Vision, from Tenets to Operational Baseline

The final set of documents is the "Operational Baseline," which looks to the past and describes the currently fielded products and their operational rules, configurations, and best practices. Like the implementation baseline, this operational baseline identifies shortcomings in security and capability. It quantifies the security risks and provides forms of mitigation that may reduce that risk. It can also provide an upgrade approach through the implementation baseline for current software that will bring it more in line with the target baseline. The operational baseline can be used to set budgets and provide support for vulnerability mitigation work. It is understood that these products probably do not meet the future goals, so the focus is on how these products are being used to best conform to the goals as described in the future-looking documents.

Figure 2 describes the overall vision. It starts at its core with the tenets, which are represented by solid rocks that are difficult to move or change. These are surrounded by concepts, which are represented by wood, which is still solid but more flexible than the tenets. The requirements are represented by formal documents, which can be changed easily but still have significant weight attached to them.

Beyond these central ideas are the three layers of documentation, the Target Baseline, the Implementation Baseline, and the Operational Baseline. Each layer is primarily related to and affected by the neighboring layers. The Target Baseline is directly driven by the Requirements, which are a practical expression of the higher-level Concepts and ultimately the Tenets. The Implementation Baseline products are evaluated directly against the Target Baseline's Technical Profile document requirements. In addition, as products are evaluated, there is a feedback process that can adjust the Target Baseline and the Technical Profile requirements to better align them with current technology. The Operational Baseline relates to the Implementation Baseline for currently fielded products that were not previously evaluated in the Implementation Baseline. These product configurations and operational practices are documented in the Operational Baseline, and any shortcomings with respect to Implementation Baseline documents for similar products are highlighted.

Table 1 Target Baseline Documentation

#	Technical Profiles
1	Application Security Guidelines
2	Configure IDPS
3	Manage Info - Provide Digital Policy with QoS
4	Provide Access Control
5	Provide Access Control Annexes
6	Provide Authentication
7	Provide Automated Info Capture Services
8	Provide Cloud Services
9	Provide Consolidated Storage Services
10	Provide Cryptographic Services
11	Provide Data Mining Services
12	Provide Data/Info/Protocol Mediation Services
13	Provide Database Services
14	Provide Domain Name Services
15	Provide Load Balancing
16	Provide Messaging Services
17	Provide Metadata Tagging & Discovery Services
18	Provide Mobile Ad Hoc Network Services
19	Provide Monitoring Services
20	Provide Network and Application Defense
21	Provide Operating System Services
22	Provide Public Key Infrastructure Services
23	Provide Presentation Services
24	Provide Service Desk Management Services
25	Provide Streaming Media Services
26	Provide Virtualization Services
27	Provide Web Browsing
28	Provide Web Hosting
29	Provide Web Services
30	Provide Widget Services
31	Provide Ports and Protocol Policy
32	Provide Satellite Communications
33	Establish Space Time Information Correlation
34	Provide Collaboration Services
35	Provide Endpoint Device Management

#	Scenarios
1	Access Management
2	Application Hosting
3	Application Performance Management
4	Data Management and Info. Exchange
5	Data on Human Users
6	Edge Information Management
7	Elasticity
8	Enterprise Info. Management
9	Ground Segment Telem. and Command
10	Incident Response
11	Infrastructure and Application Defense
12	IT Service Management
13	Key Management
14	Leverage Digital Signature
15	Leverage Infrastructure Services
16	Mobile Enterprise
17	Mobile Enterprise Annex 1 AIDC
18	Mobile Enterprise Annex 2 Loc. Services
19	Mobile Enterprise Annex 3 Wireless
20	Mobile Enterprise Annex 4 Device Mgt
21	Mobile Enterprise Annex 5 IoT
22	Network and Precision Timing
23	Resiliency

#	Capability Profiles
1	Endpoint Management Service (CP)

Table 2 Implementation Baseline Documentation

#	Implementation Baseline Document
1	Managed Platforms .NET Baseline
2	Application Services
3	Managed Platforms Database Server Baseline
4	Enterprise Level Security (ELS) Capability
5	Managed Platforms Enterprise Resource Planning (ERP) Systems
6	Managed Platforms Java Baseline

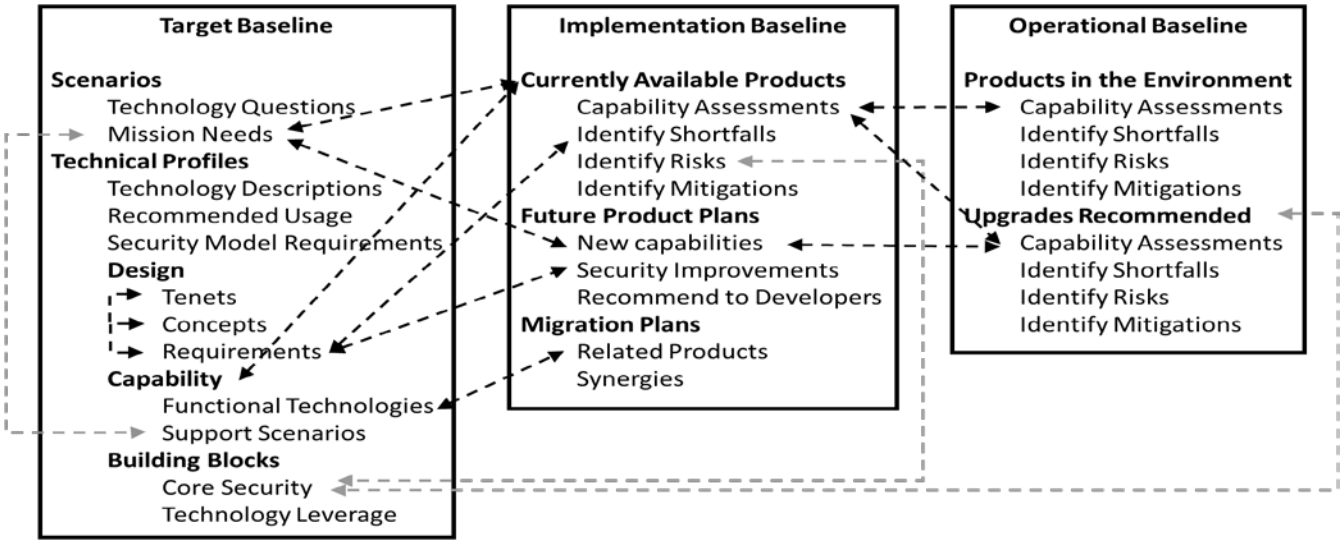

Figure 3 Documentation Hierarchy

Mitigations for vulnerabilities are also noted. Often, these are workarounds for missing capability that involve inefficiencies or security risks. By documenting these workarounds, the Implementation Baseline documents have better information about which shortcomings in current products have existing workarounds and which are fundamental problems that will require additional cost or effort. Ultimately, the Operational Baseline and the operational procedures should be driven by the Tenets, Concepts, and Requirements through this process, which keeps the entire enterprise consistent to the extent possible. Shortcomings are documented, workarounds noted, and expected compliance plans and dates are recorded.

4. REALIZING THE VISION

Scenarios include many different questions about how to perform different mission needs. The basic security model is documented in a special "Design Technical Profile" called "Application Security Guidelines." This describes the tenets, key concepts, and high-level requirements for building an ELS system. "Building Block Technical Profiles" include Authentication, Public Key Infrastructure, Access Control, and Monitoring. These apply across a large number of different capabilities and technologies. "Capability Technical Profiles" include the many technologies and capabilities that build on the core security functions to provide functionality for the enterprise.

"Capability Profiles" link the Target Baseline to the Implementation Baseline. An important question for these documents is what constitutes a capability versus a requirement. The capabilities in these documents must be described at a high enough level that they do not restrict a vendor's implementation. This allows for vendor creativity and inclusion of new technologies. However, the capabilities must be defined specifically enough that vendors cannot simply bypass key security requirements by using new and different approaches that are not proven or secure. Table 1 shows a sample list of Scenarios, Technical Profiles, and Capability Profiles.

The Implementation Baseline contains several documents. A potential set of these documents is listed in Table 2. It can be difficult to get enough information from vendors to assess their products against the fairly detailed security requirements in the Target Baseline Technical Profiles. It is tempting to simply ask the vendors if they meet all the requirements and happily accept a "Yes" answer to all such questions. However, the purpose of these documents is to provide reliable information about products, and vendors do not always provide such information freely, especially the information about requirements their products do not meet. Feedback to the groups producing target baseline documentation and education of the group writing the Implementation Baseline about current Target Baseline requirements will improve the overall evolution.

The process to perform full assessments is still under development. The need for full-time trained professionals in this area is great.

For the final component, the "Operational Baseline," the first step is to identify all current products in use. This is a considerable effort for a large enterprise, and results are often incomplete. Currently assigned personnel at the operational level do not have time to organize this aspect, and it may have to await staffing for this function. Essential feedback to both the target baseline and implementation baseline will improve the overall continuous improvement of the enterprise IT. It is expected that these documents will be very limited distribution. Figure 3 shows the relationships between the different types of documentation. The Target Baseline also describes some of its internal structure.

The dashed lines indicate paths of influence between the document types. For example, mission needs identified in scenarios shape the Capability Technical Profiles, the products analyzed for the Implementation Baseline, and the assessment of vendors' future product plans. There is mutual feedback between the capability assessments of the Implementation Baseline and Operational Baseline. Upgrades for the Operational Baseline are influenced by, and can also influence, the core security requirements in the Building Block Technical

Profiles. Many other interactions are possible. These help to keep all the documents more cohesive and relevant to each other and to current technology trends and products.

In addition to the influence between documents, the periodic discussions that follow these dashed lines help to inform owners of each document type about the other documents that are relevant. This helps to accomplish the following:

- Finding Target Baseline shortfalls in the Implementation Baseline and properly assessing associated risks.
- Finding, understanding, and assessing shortfalls, risks, and mitigations to the Operational Baseline.
- Adding necessary upgrades to the Operational Baseline, or replacing products if upgrades are not available or insufficient.
- Updating the Target Baseline to better align with current products and practices and avoid significant divergence from the commercial state-of-the-art.

5. FUTURE WORK

As the future becomes the present, we expect to see more products meeting the old requirements. The Implementation Baseline documents will be updated to reflect the current status of products with respect to the original Target Baseline. They will also be assessed against the updated Target Baseline as it evolves. For example, an Implementation Baseline document for a product may contain a history of relevant Target Baseline requirements and when they were first met. This provides information about a vendor's follow-through when promises are made to upgrade and become compliant with Target Baseline requirements.

As new products are purchased using the Implementation Baseline as guidance, these products will evolve toward the Operational Baseline as their configuration, use, and best practices are established.

Thus, with time, the Implementation Baseline and eventually the Operational Baseline will become more mature and populated with documentation. The process to track technology goals, products, and how we use them reduces the need to do a full assessment from scratch.

6. CONCLUSION

The ability to maintain a secure information system is a daunting task. We propose a systematic way to identify and document future goals, translate these to current actions, and track these over the lifetime of products in the system until they no longer meet operational needs. This requires a dedicated team to work on the future vision, another team to map this vision to currently available products, and a third to document operational procedures for current products. By maintaining these teams and fostering communication between them, it is possible to maintain the collective knowledge of an expert. The periodic review and documentation provides the stability of a bureaucracy. The mapping to current products in the Implementation Baseline and Operational Baseline ensures that these ideas track with current best practices of vendors. This approach is currently being developed and implemented, and it is evolving and maturing as more mission needs are raised, more technologies are analyzed, more products are reviewed, and the operational procedures for these products are matured and documented. This paper is part of a body of work for high-assurance enterprise computing using web services [7-13]

ACKNOWLEDGMENTS

This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). However, the publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official or unofficial position of these organizations or their members.

REFERENCES

[1] United States Labor Department, Bureau of Vital Statistics, Occupational Outlook Handbook, Computer and Information Systems Managers, April, 2018, https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm , accessed on 11 October 2018.

[2] Gino, Francesca and Staats, Bradley, "Why Organizations Don't Learn," Harvard Business Review, November 2015. Available at https://hbr.org/2015/11/why-organizations-dont-learn .

[3] Cambridge University Press, Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/bureaucracy , accessed on 11 October 2018.

[4] Johnson, Ronald N. and Libecap, Gary D., "The Federal Civil Service System and The Problem of Bureaucracy," University of Chicago Press, January 1994. Available at http://www.nber.org/chapters/c8632.pdf .

[5] Opara-Martins et al., "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective," Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:4. DOI 10.1186/s13677-016-0054-z

[6] [11]. Kevin E. Foltz and William R. Simpson, "Enterprise Level Security – Basic Security Model," 7th International Multi-Conference on Complexity, Informatics, and Cybernetics: IMCIC 2016, Orlando, Florida, March 2016.

[7] William R. Simpson, and Kevin E. Foltz, 2017. Lecture Notes in Engineering and Computer Science, "Assured Identity for Enterprise Level Security," Proceedings of the World Congress on Engineering, July 2017, Imperial College, London, pp. 440–445,

[8] William R. Simpson, and Kevin E. Foltz, 2017. "Enterprise Level Security: Insider Threat Counter-Claims," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2017, 25–27 October, 2017, San Francisco, USA, pp. 112–117.

[9] William R. Simpson and Kevin E. Foltz, 2017. Proceedings of the 22nd International Command and Control Research and Technology Symposium (ICCRTS), "Escalation of Access and Privilege with Enterprise Level Security," Los Angeles, CA. September 2017, pp. TBD.

[10] William R. Simpson and Kevin E. Foltz, 2017. Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Volume 1,

pp. 177–184, Porto, Portugal, 25–30 April, 2017, "Enterprise Level Security with Homomorphic Encryption," SCITEPRESS – Science and Technology Publications.

[11] Kevin Foltz, and William R Simpson, 2016. "Enterprise Considerations for Ports and Protocols," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2016, 19–21 October, 2016, San Francisco, USA, pp.124–129.

[12] Simpson, William R., CRC Press, 2016. *Enterprise Level Security – Securing Information Systems in an Uncertain World*, by Auerbach Publications, ISBN 9781498764452, May 2016, 397 pp.

[13] Kevin E. Foltz and William R. Simpson, 2016. Wessex Institute, Proceedings of the International Conference on Big Data, BIG DATA 2016, "Access and Privilege in Secure Big Data Analysis," 3–5 May 2016, Alicante, Spain, pp. 193–205.