
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**RULES AND A RUBRIC COULD BE USED TO ASSESS THE OPENNESS OF A HOMELAND SECURITY ENTERPRISE SOCIAL NETWORK**

by

Jeffrey Thomas Murray

December 2016

Thesis Co-Advisors: Nadav Morag
Paul Smith

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503. | | | |
| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** December 2016 | **3. REPORT TYPE AND DATES COVERED** Master's thesis | |
| **4. TITLE AND SUBTITLE** RULES AND A RUBRIC COULD BE USED TO ASSESS THE OPENNESS OF A HOMELAND SECURITY ENTERPRISE SOCIAL NETWORK | | | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Jeffrey Thomas Murray | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | | **10. SPONSORING / MONITORING AGENCY REPORT NUMBER** |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release. Distribution is unlimited. | | | **12b. DISTRIBUTION CODE** |

**13. ABSTRACT (maximum 200 words)**


The Homeland Security Enterprise (HSE) lacks a process to create a body of knowledge to unify its stakeholders. This thesis asked if a set of rules and an assessment methodology could be applied to three wikis to illustrate how the rules can improve the quality of information-sharing across the HSE.

The research for this thesis applied a set of rules and an assessment methodology to case studies testing the hypothesis that wikis are a good example of an enterprise social network (ESN) and could serve to meet the information needs of the HSE. The methodology will apply Bloom's Taxonomy to a rubric and establish a current status, as well as plan a path ahead for development.

This thesis investigated the demand for improved information sharing and some existing platforms, and developed an assessment rule set and rubric. It then discovered the openness strengths and weaknesses of three case studies using the rules and rubric. Our conclusions are that the rules and rubric are adequate to develop paths to improvement for existing platforms, as well as to aid in the planning of future ESNs with the intention of developing a wiki-based homeland security-centric ESN designed to create an HSE body of knowledge.


| **14. SUBJECT TERMS** information sharing, crowdsourcing, collective intelligence, wiki, enterprise social network, and rubric | | | **15. NUMBER OF PAGES** 109 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

**RULES AND A RUBRIC COULD BE USED TO ASSESS THE OPENNESS OF A HOMELAND SECURITY ENTERPRISE SOCIAL NETWORK**

Jeffrey Thomas Murray
Protective Security Advisor, Office of Infrastructure Protection,
United States Department of Homeland Security, Albuquerque, New Mexico
B.S., Liberty University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2016**

Approved by: Nadav Morag
Thesis Co-Advisor

Paul Smith
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

The Homeland Security Enterprise (HSE) lacks a process to create a body of knowledge to unify its stakeholders. This thesis asked if a set of rules and an assessment methodology could be applied to three wikis to illustrate how the rules can improve the quality of information-sharing across the HSE.

The research for this thesis applied a set of rules and an assessment methodology to case studies testing the hypothesis that wikis are a good example of an enterprise social network (ESN) and could serve to meet the information needs of the HSE. The methodology will apply Bloom's Taxonomy to a rubric and establish a current status, as well as plan a path ahead for development.

This thesis investigated the demand for improved information sharing and some existing platforms, and developed an assessment rule set and rubric. It then discovered the openness strengths and weaknesses of three case studies using the rules and rubric. Our conclusions are that the rules and rubric are adequate to develop paths to improvement for existing platforms, as well as to aid in the planning of future ESNs with the intention of developing a wiki-based homeland security-centric ESN designed to create an HSE body of knowledge.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ALA | American Library Association |
| BoK | body of knowledge |
| CSAI | Center on Standards and Assessment Implementation |
| CIA | Central Intelligence Agency |
| CRS | Congressional Research Service |
| DHS | Department of Homeland Security |
| DoJ | Department of Justice |
| DNI | Director of National Intelligence |
| ESN | enterprise social network |
| EO | Executive Order |
| FBI | Federal Bureau of Investigation |
| FOUO | For Official Use Only |
| GAO | Government Accountability Office |
| HS | homeland security |
| HSE | homeland security enterprise |
| IO | information operations |
| ISAO | information-sharing and analysis organization |
| ISC | Information-sharing Council |
| ISE | Information-sharing Environment |
| IC | intelligence community |
| IRTPA | Intelligence Reform and Terrorism Prevention Act of 2004 |
| ISIL | Islamic State of Iraq and the Levant |
| JISTF | Joint Information-sharing Task Force |
| LE | law enforcement |
| MIT | Massachusetts Institute of Technology |
| NCTC | National Counterterrorism Center |
| NCCIC | National Cybersecurity and Communication Integration Center |
| NPOV | neutral point of view |
| I&A | intelligence and analysis |
| PCLOB | Privacy and Civil Liberties Oversight Board |

| | |
|---|---|
| PM-ISE | Program Manager-Information-sharing Environment |
| QHSR | Quadrennial Homeland Security Review |
| SLTT | state, local, tribal, and territorial |
| SC | strategic communication |
| SME | subject matter expert |
| SAR | suspicious activity reporting |
| USIC | U.S. Intelligence Community |
| USPTO | U.S. Patent and Trademark Office |
| WMD | weapons of mass destruction |

# EXECUTIVE SUMMARY

This thesis has established the continued demand for improved information sharing by lawmakers and policymakers. Attempts have been made, but a common homeland security (HS)-centric information-sharing platform still does not exist. The homeland security enterprise (HSE) is far larger than just the federal agencies or just law enforcement (LE) or just the U.S. intelligence community (IC). The HSE spans across all levels and most disciplines of the government and includes the private sector as well.

The threats to the homeland continue to diversify and increase in complexity, which reinforces the need for increased connectedness across the HSE. Another consideration related to the HSE is the need for a body of knowledge (BoK) to reinforce HS as a discipline. Despite these demands and the absence of a comprehensive platform for well over a decade, senior leadership across the HSE has not provided or recommended a viable approach. This thesis has attempted to address this need.

The literature related to this problem illustrates the persistent demand for getting "the right information to the right people at the right time," while not naming a specific approach to address this demand. There is no shortage of laws to include the PATRIOT Act, executive orders, strategic plans, and independent studies by Government Accountability Organization (GAO) and the Congressional Research Service (CRS) directing agencies and organizations to find a way to attempt to meet these demands.

The continued demands and the associated inadequate attempts are beginning to result in a kind of information-sharing apathy from all the participants. This apathy is concerning because most likely it can revitalize the mentality of "need to know" at the expense of "need to share." This mentality could reasonably result in information blindness prior to the next significant HS incident.

This thesis looks to the concept of collective intelligence as an approach to connecting the HSE. This well-established approach to gathering information through the use of crowdsourcing could be an effective approach. By decentralizing the sources of information, and making that information available across the HSE, has a high

probability of success. Basing this process on an ESN could bring necessary structure to this approach. This thesis has used a wiki as a viable ESN option.

This theory to unify the HSE will need some rigor to be accepted as a viable option by legislators and policymakers to allocate additional resources, and this thesis proposes a set of rules and a rubric based on well-established knowledge management and assessment research. The rules are (1) allow cultural change over time, (2) create opportunities for people to get to know one another, (3) focus on connecting people vice capturing content, (4) provide top-down support of bottom-up solutions, (5) serve as positive role models wherever possible, and (6) consistently reward knowledge sharing behavior.

The rules in and of themselves are not enough to provide sufficient guidance to the assessment or establishment of an ESN. The rules also require a rubric to serve as a guide for ESN planners to improve existing and create new ESNs. The ESN rubric employs Bloom's Taxonomy as a guide to assessing the maturity of an ESN. For each rule, the rubric applies the six gradations on Bloom's Taxonomy: remembering, understanding, applying, analyzing, evaluating, and creating along with a point system so that the ESN can receive a score for each rule, as well as a cumulative score.

Three ESNs served as case studies to validate this approach. All the ESNs are wikis and they are the ubiquitous Wikipedia, the USPTO's Peer-to-Patent and the DNI's Intellipedia. The background of the cases was discussed and then the rubric was applied to each of them that resulted in a maturity score for each of them. Wikipedia scored the highest followed by Intellipedia and then Peer-to-Patent.

The purpose of the BoK that would be the HSE ESN is to connect the lesser-known members of the HSE that have and can benefit from access to valuable unclassified information to other members of the HSE to include the LE and ICs.

This thesis has made possible significant improvements in the information-sharing process across the HSE by creating a simple and actionable assessment methodology. This process will hopefully keep the HSE engaged in the pursuit of optimal

connectedness to avert or at least effectively respond to the wide range of threats facing the homeland.

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I would like to thank my wife, Alison, for her support and patience through the entire program. It would not have been possible without her. I would like to thank my advisors, Nadav and Paul, for their continuous guidance, support, and insight through this process. I am grateful to the faculty and staff of the Naval Postgraduate School and the Center for Homeland Defense and Security (CHDS) for their professionalism, commitment to my success, and patience through this program. Lastly, I would like to thank Chris Bellavita and Lauren Wollman for their well-timed sage words of wisdom. They are a priceless part of CHDS.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

The United States has more than 18,000 law enforcement (LE) agencies,[1] 30,000 fire departments,[2] and 5,000 hospitals.[3] Eighty-five percent of the United States' critical infrastructure is privately owned.[4] None of these communities has a centralized coordination system. They all have their own control and communication structures within their respective jurisdictions and few of them collaborate. Yet, they all have a role in preparing for, preventing, mitigating, responding to, and recovering from any number of threats. Information sharing will be vital in coordinating and collaborating with those stakeholders.

The Director of National Intelligence (DNI) presents the *Worldwide Threat Assessment* annually to Congress. It lists and prioritizes the threats facing the United States according to U.S. Intelligence Community (USIC). The 2016 Assessment names cyber and technology, terrorism, weapons of mass destruction, space and counterspace, counterintelligence, transnational organized crime, economic and natural resources, and human security as the greatest threats to the United States[5] This broad spectrum of threats has the potential to affect all levels of government and the private sector. It is unlikely that every organization has or can afford an experienced generalist who can provide credible, accurate, and timely information on all these threats.

Information availability is essential to the homeland security enterprise (HSE). Legislators and policy makers have demanded constant improvements to information sharing for nearly two decades. The call for improved information sharing has also been

---

[1] Brian A. Reaves, "Bureau of Justice Statistics (BJS)," Census of State and Local Law Enforcement Agencies, July 26, 2011, http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2216.

[2] Michael J. Karter, Jr. and Gary P. Stein, "U.S. Fire Department Profile," National Fire Protection Association, October 1, 2013, http://www.nfpa.org/research/reports-and-statistics/the-fire-service/administration/us-fire-department-profile.

[3] "Fast Facts on U.S. Hospitals," January 2, 2014, http://www.aha.org/research/rc/stat-studies/fast-facts.shtml.

[4] U.S. Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* (GAO-07-39) (Washington, DC: U.S. Government Accountability Office, 2006), http://www.gao.gov/products/GAO-07-39.

[5] James C. Clapper, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington DC: Office of the Director of National Intelligence 2016), ii.

picked up by organizations like the International Association of Law Enforcement Intelligence Analysts,[6] the International Association of Chiefs of Police,[7] the National Fusion Center Association,[8] and the International Association of Fire Chiefs.[9] These groups are combining their demands as evidenced by Boston Police Commissioner Edward Davis' testimony to the U.S. House of Representatives where he continued to emphasize the importance of information sharing.[10]

The existing platforms have made significant improvements in information sharing but none allow for broad distribution and quick collaboration. Establishing a simple set of rules to be applied to existing and future information-sharing platforms designed to improve their effectiveness could dramatically improve the connectedness of the HSE across a wide variety of disciplines.

## A. PROBLEM STATEMENT

The HSE does not have a process to build and assess a body of knowledge (BoK) to unify the extraordinarily disbursed and varied stakeholders. Federal, state, local, tribal, territorial and private sector entities need to be more informed, unified, and connected beyond what current information-sharing platforms have to offer. No accepted rule set exists that can be used to evaluate and guide the development and execution of new platforms.

## B. EVIDENCE OF INFORMATION-SHARING FAILURE

Historically, federal, state, and local responders have shared information inconsistently. If a system had existed, it was based on established relationships versus an

---

6 "Mission," accessed November 20, 2016, http://www.ialeia.org/about-us/mission.html.

7 International Association of Chiefs of Police, *Strategic Plan* (Alexandria, VA: International Association of Chiefs of Police, 2010), 17, http://www.iacp.org/portals/0/pdfs/IACPStrategicPlan.pdf.

8 "Home," accessed November 20, 2016, https://nfcausa.org/default.aspx/MenuItemID/135/MenuGroup/Public Home.htm.

9 "EMR-ISAC: A Critical Information-Sharing Tool," October 15, 2011, http://www.iafc.org/MemberCenter/OnSceneArticle.cfm?ItemNumber=5184.

10 U.S. House of Representatives, *Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security* (Washington, DC: U.S. House of Representatives, 2013), 3, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-DavisE-20130509.pdf.

organized system or process. The *9/11 Commission Report* (the Report) revealed a statutorily imposed "wall"[11] between LE and the intelligence community (IC) on the premise of preventing spying on U.S. citizens.[12] The legislative branch's investigation, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*, found a systemic failure, "Serious problems in information-sharing also persisted, prior to September 11, 2001 between the intelligence community and relevant non-intelligence community agencies. This included other federal agencies as well as state and local authorities."[13]

The Commission identified information sharing as a priority to preventing attacks similar to what occurred on September 11, 2001. In Chapter 13, Section 3 of the Report, the Commission recommends, "Information procedures should provide incentives for sharing, to restore a balance between security and shared knowledge," meaning information that can be shared across organizations must be processed for dissemination while protecting sources and methods."[14] The federal government produced policies and procedures to support information sharing across agencies at all levels of government (federal, state, local, tribal and territorial) and the private sector as a result.

The primary policy on information sharing is the 2012 *National Strategy for Information-sharing and Safeguarding*. The policy maxim is "Our national security depends on our ability to share the right information, with the right people, at the right time;"[15] easier said than done, especially when the strategy does not define the terms "right," "information," "people," or "time." Subsequently, many agencies have created

---

[11] The term "the wall" was used in the report in reference to the Foreign Intelligence Surveillance Act (FISA) regulating the collection of foreign powers and agents in the United States, found on page 78 of the report.

[12] Richard A. Best Jr., *Sharing Law Enforcement and Intelligence Information: The Congressional Role* (CRS Order Code RL33873) (Washington, DC: Congressional Research Service, 2007).

[13] U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001* (Washington, DC: U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, 2002), 29, http://fas.org/irp/congress/2002_rpt/911rept.pdf.

[14] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2011), 417.

[15] White House, *National Strategy for Information-sharing and Safeguarding* (Washington, DC: White House, 2012), 1.

their own information-sharing organizations and systems—whether physical or virtual—which, while meeting the strategy objectives, are written to protect agency interests.

These structures have met with varying degrees of success. No single platform provides consistent over-arching homeland security (HS) information for the varied population of the HSE. The most promising information-sharing platform, based on the same concept as the extremely successful Wikipedia,[16] is Intellipedia. Not without its own difficulties, Intellipedia is only open to the IC and is experiencing stagnation in growth and participation.[17] Intellipedia is reviewed in greater detail in the case studies chapter.

## C. PROBLEMATIC NATURE OF INFORMATION-SHARING

For the sake of clarity, the HSE is defined in this paper as the federal, state, local, tribal and private sector entities that require coordination and are involved in securing against and responding to all-hazard threats without implying total protection or complete threat mitigation.[18]

It is important to explore significant intelligence failures like those associated with the 9/11 attacks,[19] the Boston marathon bombing,[20] or any other low probability-high-impact[21] incidents. It is more important to explore routine coordination across the HSE where the lines of communication are established and maintained, as well as where

---

[16] "Wikipedia is a free encyclopedia, written collaboratively by the people who use it. It is a special type of website designed to make collaboration easy, called a wiki. Many people are constantly improving Wikipedia, making thousands of changes per hour. All of these changes are recorded in article histories and recent changes," *Wikipedia*, s.v. "Introduction," last modified September 10, 2015, http://en.wikipedia.org/wiki/Wikipedia:Introduction.

[17] Joab Jackson, "Intellipedia Suffers Midlife Crisis," *Government Computer News*, February 18, 2009, http://gcn.com/Articles/2009/02/18/Intellipedia.aspx.

[18] Shawn Reese, *Defining Homeland Security: Analysis and Congressional Considerations* (CRS Report No. R42462) (Washington, DC: U.S. Congressional Research Service, 2013), 9, http://www.fas.org/sgp/crs/homesec/R42462.pdf.

[19] The 9/11 Commission Report cites a lack of information sharing between law enforcement and intelligence organization as a contributing factor to the success of the attacks.

[20] A Department of Justice report on the information sharing and handling surrounding the Boston marathon bombing found errors was made in sharing identity information between law enforcement and the intelligence community.

[21] A low probability-high impact event is one that may not occur very often but when it does, it is very disruptive.

a significant amount of information sharing is conducted. It is not necessarily one singular piece of datum that makes a significant contribution to overall HS but a vast amount of information shared across a wide variety of connected stakeholders that has tremendous impact.

The continuous development of a large BoK shared across a wide spectrum of consumers can make the most significant contribution to information sharing. Simply put, it is valuable to create an adaptive, large-scale collaborative environment, also known as an enterprise social network or ESN, available to all members of the HSE. Vital components of that ESN are rules that guide cultural development within that environment and an assessment methodology or rubric to illustrate to what degree those rules are being followed.

All incidents experience faults in information sharing, usually documented in hindsight. A common lament involves discovering one entity knowing or needing a critical piece of information and not knowing another entity had or needed it. A good first step is evolving away from a "need-to-know" mentality to one of "need-to-share." What seems like a simple step is arguably the most difficult. Information sharing is different from traditional intelligence-driven operations. Intelligence operations typically use specific collection platforms looking for particular information to form a more focused picture to act upon by distinct operational assets. Information sharing is more amorphous than intelligence operations in the sense that it comes from a wide variety of sources and is intended for a similarly wide audience.

The result is an unorganized flow of information to an unorganized group of consumers. Those who generate information tend to limit distribution to those within a small group, usually only those within their network. Although the generator may want to disseminate the information further, an intended audience may not be adequately identified and developed. Additionally, those seeking information may suffer from limited access to needed information, and therefore, rely on limited information from known contacts or extensive information from uncertain sources.

This disorganization is degrading the ability of the broad spectrum of participants in the HSE to collaborate, educate those new to HS, and maintain a centralized and

current BoK. Without the ability to collaborate with a wide variety of mission partners to include public health officials and the private sector, first responders will find it increasingly difficult to accomplish their missions.

This thesis proposes a rule set and an assessment methodology to be used to improve the development of ESNs.

## D. RESEARCH QUESTION

How can a rule set and assessment methodology be applied to existing and new information-sharing platforms to improve their effectiveness, and ultimately, improve the connectedness of the HSE?

## E. HYPOTHESIS

The success of Wikipedia in collectively assembling information on any given topic of interest via shared authorship could be a practical model to unify the HSE. This model differs from finished intelligence products that are typically classified because they are attributed to specific sources and methods. By inspiring members to share their general knowledge and expertise on particular subjects, with oversight and over time, a BoK for the HSE would evolve using an ESN. A simple rule set and assessment methodology could provide structure and boundaries for that evolution.

The rules should shift focus away from connecting organizations or collecting bits of data and redirect it to connecting people in a more substantial and sustainable way. An assessment methodology needs to go beyond a simple "pass or fail." It should be constructed in such a way as to provide not only a useful view of where an ESN is relative to the rule set but also provide a direction for future growth utilizing the rule set.

For example, the Department of Homeland Security (DHS) could sponsor an ESN in the form of a wiki to unite all vetted users to share information in a structured way to form a HSE BoK. The rule set could be applied during the planning phase to better ensure key components of an ESN are being addressed. The assessment methodology could then be employed periodically over the life of the ESN to maintain effectiveness.

## F. METHODOLOGY

The research for this thesis applies a simple set of rules and an assessment methodology to case studies of the ubiquitous Wikipedia, the U.S. Patent Office's Peer-to-Patent wiki and Office of the Director of National Intelligence's Intellipedia. This research tests the hypothesis that wikis are a good example of a formidable ESN and could serve to meet the broad general information needs of the HSE.

The rules themselves are derived from established information sharing and knowledge management research. They support the intent of the hypothesis by focusing on those components that bring the members of the HSE together in a collaborative ESN. The rules address the topics of culture, connectedness, leadership support, mentorship, and incentives.

The methodology applies Bloom's Taxonomy to create depth within the rules and establish pathways associated with each of the rules so existing ESNs can see their current status, as well as plan a path ahead for development. The rules and the assessment also, and arguably more importantly, assist with the planning of a future HS ESN with the intent to connect the HSE in the broadest sense possible and achieve two significant goals. The first goal is to create an ever-growing and updated BoK and the second is to provide a platform for subject matter experts (SMEs) to have a centralized platform to share validated and timely information.

This thesis is designed to address these topics. This introduction is followed by a literature review to establish some background on the demands for information sharing and discuss the concepts of collective intelligence, crowdsourcing, ESNs, and wikis. The next chapter then establishes and discusses the rules and the rubric, which is followed by a series of case studies that provide some background and apply the rules and rubric to them. Lastly, findings and a conclusion are provided.

## G. CONCLUSION

Accurate and coordinated information must be made available to the HSE to effectively combat the myriad and evolving threats to the homeland. Using a more comprehensive collective intelligence-based ESN, possibly a wiki, the federal

government could more effectively support collaboration across the HSE. This thesis explores the value of applying a simple set of rules and an associated assessment methodology to ESNs to monitor the quality of their sharing of information.

The following literature review explores the demands made by Congress to constantly improve information sharing, the policies the executive branch has created to meet those demands, and an examination of collective intelligence, crowdsourcing, and wikis as a collaboration method.

# II. LITERATURE REVIEW

To this point, this thesis has discussed the problems facing information sharing, the multitude of threats facing the HSE, theorized the benefits of establishing a homeland BoK, and established a research question to guide inquiry. This literature review focuses on legislation and policy that regulates and guides information sharing. It also considers the criticism surrounding those laws and policies.

The next section provides some necessary background to establish the continued demand by legislators and policymakers to improve information sharing continuously while providing minimal guidance. The information-sharing philosophy changed significantly in 2009. *The Modern Era* takes a detailed look at that philosophical change, legislation, policy, and critique from 2009 to 2016. *Collective Intelligence* explores the capabilities and limitations of this information-sharing and collaboration approach. *Crowdsourcing* outlines specific qualities of this collective intelligence-based collaboration approach and focuses on the development of a BoK.

## A. BACKGROUND

Executive Orders (EOs) bridge the gap between legislation and policy. The National Archives define executive orders as, "official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government."[22]

The Government Accountability Office (GAO) and the Congressional Research Service (CRS) perform audits of federal government activities on behalf of Congress. These reports help to monitor programs and inform the legislative branch of potential issues. Information sharing has been a regular topic of study for both organizations.

The Markle Foundation has produced some very influential policy recommendations and is a non-profit organization dedicated to developing policy support

[22] "FAQ's About Executive Orders," accessed August 13, 2014, http://www.archives.gov/federal-register/executive-orders/about.html#orders.

in the areas of national security technology.[23] It created the Task Force on National Security in the Information Age that produced a series of reports in collaboration with former policy makers from previous presidential administrations, information technology executives, and privacy and civil liberty advocates who had been influential in the development of current policy.[24]

Information sharing came to the fore as a topic of legislation in 1996. It started with the Aspin/Brown Commission referring to terrorism and narcotics trafficking as "global crime," and requiring LE and intelligence enterprises to work more closely on solving these problems.[25] The Aspin/Brown Commission recommended interagency working groups to share information to address these issues.[26]

Following the attacks of 9/11, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was signed into law in October 2001 and to empower LE to pursue those responsible for the attacks.[27]

The *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* cited, "a range of political, cultural, jurisdictional, legal and bureaucratic are ever-present hurdles to information-sharing."[28] For the first time, a comprehensive review was conducted across the HSE accompanied by specific recommendations applicable across all federal agencies.

---

[23] "National Security," accessed December 5, 2016, https://www.markle.org/national-security.

[24] "Markle Task Force on National Security," accessed December 5, 2016, https://www.markle.org/national-security/markle-task-force-national-security.

[25] Harold Brown and Warren B. Rudman, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Darby, PA: Diane Publishing, 1996), 37.

[26] Ibid.

[27] Charles Doyle, *The USA PATRIOT Act: A Legal Analysis* (CRS Order Code RL31377) (Washington, DC: Congressional Research Service, 2002), 2.

[28] Bob Graham and Richard C. Shelby, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001* (Washington, DC: Senate Intelligence Committee, 2002), 4, http://www.intelligence.senate.gov/pdfs/1071086v2.pdf.

The Homeland Security Act of 2002 (HSA 2002), passed in October 2002, created the DHS and tasked it with a wide variety of missions. The Act required the DHS to improve information sharing across all levels of government and the private sector.[29]

The USA PATRIOT Act, The Joint Inquiry, and HSA 2002, were all created following the attacks of 9/11 but prior to the establishment of the DHS as an organization. These laws and policies created the theory of the DHS and provided the thought behind what HS is and does.

The Report was the seminal report and driving force behind legislation and policy influencing HS related information sharing.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the DNI, National Counterterrorism Center (NCTC), the Privacy and Civil Liberties Oversight Board (PCLOB), the Information-sharing Environment (ISE), the Program Manager-Information-Sharing Environment (PM-ISE) and the Information-sharing Council (ISC).[30] IRTPA created the information-sharing structure of the federal government, and in doing so, made information sharing a government priority. IRTPA also added civil rights and civil liberties to information-sharing requirements.[31]

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (The WMD Commission) recommended the consolidation of authority and management concerning intelligence information and recommended the clarification of the chain of command for the PM-ISE as a subordinate to the DNI but answerable to the President.

The main information-sharing EO is 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans,* and was issued in October 2005. It ordered the Executive Branch to design information systems to share terrorism information across

[29] "Bill Summary & Status 107th Congress (2001–2002) H.R. 5005 CRS Summary," accessed June 26, 2014, http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05005:@@@D&summ2=m&.

[30] "The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)," accessed July 24, 2014, https://it.ojp.gov/default.aspx?page=1282.

[31] Ibid.

the HSE.[32] It enhanced and amended the National Security Act, the Homeland Security Act, the IRPTA, and EOs 12958, *Classified National Security Information*, and 13311, *Homeland Security Information-sharing*, revoked EO 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans*.[33]

*Implementing Recommendations of the 9/11 Commission Act of 2007 (The 9/11 Commission Act)* amended the IRTPA and the Homeland Security Act of 2002 to improve the scope of the ISE and define HS information, the information-sharing environment, terrorism information, and WMD information.[34] Most importantly, it was the last significant piece of information-sharing legislation. No new legislation has addressed information sharing in nearly nine years.

The 2007 GAO report titled, Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives, observed that the DHS and the Department of Justice (DoJ) used 17 major networks to support HS related missions.[35] This capability came at a cost of almost 500 million dollars a year.[36] This report was the most significant assessment of the federal government's efforts to share information. It made the point that too many organizations were spending far too much to achieve very little when it came to information sharing.

As the "modern era of information sharing" approaches, an exorbitant amount of money, time, and effort has been expended without any information-sharing policy or structure appearing to answer the demands of legislators or policy makers. The HSE information-sharing environment has struggled to achieve the level of proficiency necessary to be deemed successful.

---

[32] George W. Bush, "Executive Order 13388," Federation of American Scientists, October 25, 2005, http://www.fas.org/irp/offdocs/eo/eo-13388.htm.

[33] Ibid.

[34] "The Implementing Recommendations of the 9/11 Commission Act of 2007," accessed July 24, 2014, https://it.ojp.gov/default.aspx?page=1283.

[35] David A. Powner, *Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives* (GAO-07-455) (Washington, DC: Government Accountability Office, 2007), 2, http://www.gao.gov/assets/260/259384.pdf.

[36] Ibid., 4.

## B. THE MODERN ERA (FROM 2009 TO 2016)

Significant information-sharing policy development has occurred since 2009. A variety of organizations have released guidance not only to improve information sharing but also to protect privacy and civil liberties in the process. The following section reviews those policies and highlights critiques of those policies.

Following the change of administration in 2009, the Markle Foundation released *Nation at Risk: Policy Makers Need Better Information to Protect the Country* in March 2009. It emphasized the importance of the best information being discoverable and accessible to policymakers by using technology to achieve that goal and lessening "bureaucratic resistance to change."[37] *Nation at Risk* was followed by *Meeting the Threat of Terrorism: Culture Change* in September 2009, which recommended the administration emphasize the use of clear guidance and incentives to change behavior in recommendations to the new administration.[38]

It recommended emphasizing the importance of personnel in addition to technology as opposed to instead of it, and prioritizing and incentivizing a "need to share" mentality. Another important concept introduced in the Report emphasizes balancing sharing information while at the same time protecting it.[39] This theme will be recurring throughout upcoming reviewed policy and critiques to connect people and establish a culture of "need to share" securely while respecting civil rights and privacy.

In February 2011, the DHS Office of Intelligence and Analysis (I&A) issued its strategic plan designed to last through 2018. The plan consisted of four goals, to apply intelligence analysis to understand threats better, collect HS related information, share actionable information, and manage intelligence for the HS enterprise.[40] A significant

---

[37] "Nation At Risk: Policy Makers Need Better Information to Protect the Country," March 1, 2009, http://www.markle.org/publications/487-nation-risk-policy-makers-need-better-information-protect-country.

[38] "Meeting the Threat of Terrorism: Culture Change," September 1, 2009, http://www.markle.org/publications/499-meeting-threat-terrorism-culture-change.

[39] Ibid.

[40] U.S. Department of Homeland Security, *Office of Intelligence and Analysis Strategic Plan* (Washington, DC: U.S. Department of Homeland Security, 2011), 7, http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf.

contribution of the strategy was defining the HSE as, "all of I&A's stakeholders in the Department; the Intelligence Community; the private sector; and SLTT governments."[41] This statement serves to define the broad range of stakeholders that contribute to protecting the homeland and especially those outside the control of the federal government.

The DNI issued the *Strategic Intent for Information-sharing* in August 2011. This brief document outlined the goals and objectives of the USIC as it applies to information sharing. The document lists five goals: optimize the sharing of information and intelligence within the IC and with partners and customers to enable decision advantage; maximize and integrate IC capabilities to discover, access, retain, store, share, and exploit information; maximize and integrate IC capabilities to secure information; review, align, and strengthen the governance framework to optimize responsible information sharing, while protecting civil liberties and privacy; and promote a culture of responsible information sharing.[42]

As would be expected from a strategic intent document, very little appears in the way of explaining how to accomplish the goals and objectives, which tends to allow organizations to interpret their approaches as they see fit to answer their own needs. It does not necessarily lead to meeting the expanding needs of the HSE. The HSE would benefit from direction from the DNI on what approach should be taken to meet the aforementioned goals, or at a minimum, a way to assess if it is meeting those goals. The ambiguity of this policy could easily lead to wasted resources when organizations use disparate platforms to share information with anyone other than themselves.

In the 2011 GAO report titled, *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*, a key finding was "The government continues to make progress in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning Information-sharing Environment (ISE) in

[41] U.S. Department of Homeland Security, *Office of Intelligence and Analysis Strategic Plan*, 6.

[42] Office of the Director of National Intelligence, *Strategic Intent for Information-sharing* (Washington, DC: Office of the Director of National Intelligence, 2011), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/11152526_strategic_intent_info_sharing.pdf.

place."[43] Despite continued policy documents, legislation, and financial outlay, the ISE is not meeting the information needs of stakeholders. Part of this shortfall can be explained by the lack of an actual environment. No one space is available where all HSE partner's information can exist for the benefit of the rest of the enterprise.

The CRS released a report in 2011 titled, *Intelligence Information: Need-to-Know vs. Need-to-Share*, which discussed the challenges to sharing information and the associated risks should that information be improperly released.[44] The report reviewed significant information-sharing issues related to the Detroit bombing attempt, the Fort Hood shootings, and the Wikileaks incident.

The Report focused on the information-sharing shortcomings in each of these case studies. The Detroit bombing attempt involved Umar Farouk Abdulmutallab's attempt to detonate explosives concealed in his underwear on a flight into Detroit from Amsterdam. The Fort Hood shootings involved U.S. Army Major Nidal Hasan shooting 45 service members and one civilian on Fort Hood, killing 13.[45] In both of these incidents, the report found a failure to share available information between agencies, a failure to analyze disparate information effectively, and a failure to notify responsible officials effectively to contributing factors in these cases.[46]

This type of failure is a persistent challenge with information sharing. Organizations frequently do not realize or are unwilling to admit they are in possession of information that is necessary for another organization to be successful in their mission. It would seem a single place where organizations can place general information that can provide vital pieces of the puzzle for other organizations would be a very practical demand from legislators and policy makers. More importantly, providing some structure

---

[43] Eileen R. Larence, *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information* (GAO-12-144T) (Washington, DC: Government Accountability Office, 2011) 8, http://www.gao.gov/assets/590/585711.pdf.

[44] Richard A. Best Jr., *Intelligence Information: Need-to-Know vs. Need-to-Share* (CRS Report No. R41848) (Washington, DC: Congressional Research Service, 2011), https://www.fas.org/sgp/crs/intel/R41848.pdf.

[45] Ibid., 9.

[46] Ibid., 10.

and a means to measure effectiveness would make that approach more sustainable and resilient.

The Report then made an extraordinarily important assertion by trying to emphasize that "need-to-know" or "need to share" is a false choice. Information must always be shared but the people with access to that information need to be vetted effectively and efficiently and accountability must be associated with that access. Approaches to improving sharing like the practice of "tear lines" to refine classified information to a reduced "shareable" form have value although they are cumbersome and rely on the originator to want to share specific information. Effective intelligence efforts are never risk-free and the government needs to accept a media culture that considers disclosure a patriotic contribution.[47] It is an important precedent set by CRS. The perception of being able to control information and still effectively share it is flawed because both objectives cannot be achieved simultaneously.

Finally, the Report stated the ISE is understaffed and attempts to establish consistent policy guidelines across the defense, intelligence, HS, foreign affairs, and LE communities.[48] It needs a more efficient method for not only sharing information but collaboration as well. This idea tends to get lost in the policy discussion.

Another significant CRS report released in 2011 titled, *Terrorist Use of the Internet: Information Operations in Cyberspace*, illustrated the many ways terrorist organizations have leveraged the internet to accomplish important tasks like radicalization and recruitment, propaganda distribution, communication, and training.[49] This leverage is a key observation. U.S. opponents are quickly adopting the new internet-based communication and collaboration platforms to advance their objectives and accomplish their missions while the HSE is not.

The Report also illustrated challenges facing the U.S. government in addressing these capabilities. It listed over-classification, interagency competition, poor information

---

[47] Best, *Intelligence Information: Need-to-Know vs. Need-to-Share*, 13.

[48] Ibid., 6.

[49] Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace* (CRS Report No. R41674) (Washington, DC: Congressional Research Service, 2011), 2, http://www.fas.org/sgp/crs/terror/R41674.pdf.

sharing, legislative misinterpretation, inconsistent agency approaches to addressing the issues, and differing strategies for information operations (IO) and strategic communication (SC) as issues needing to be addressed by Congress.[50] The CRS is clearly illustrating the failures of existing legislation and policies to guide information sharing within and among the HSE. It is exasperating to review these persistent challenges and realize that they could lead to complacency and an acceptance of information sharing being just too complicated a problem when it actually is not.

The National Infrastructure Advisory Council produced a report titled, *Intelligence Information-sharing-Final Report and Recommendations*, in January 2012. The report made recommendations to both the federal government to include the USIC, as well as the private sector.[51] Among the recommendations were increasing the importance of critical infrastructure related information to the USIC, improving the combined collaborative analysis capability between the USIC and the private sector, developing incentives to improve public/private partnerships, streamlining the federal intelligence-sharing process and improving the DHS' role as a champion for critical infrastructure information sharing.[52]

These recommendations were a first step in improving awareness of the need to include the private sector in information sharing. Critical infrastructure is vital to this country's national security. It is predominantly owned and operated by the private sector and it needs the support of the USIC to address threats. It also possesses extensive information that can support the HSE. A HS ESN, possibly in the form of a wiki, could address the recommendations in this report.

In December 2012, the White House issued the *National Strategy for Information-sharing and Safeguarding* (the Strategy). It coined the phrase in the first line of the executive summary, "Our national security depends on our ability to share the right

---

[50] Theohary and Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace*, 12.

[51] U.S. Department of Homeland Security, *Intelligence Information-sharing Final Report and Recommendations* (Washington, DC: U.S. Department of Homeland Security, 2012), http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[52] Ibid., ES-2.

information, with the right people, at the right time."[53] This sentence is regularly quoted in other information-sharing related material and is frustrating to information-sharing practitioners in its simultaneous obviousness and vagueness. No one would argue with this guidance yet few know how to accomplish it.

The Strategy established the principles of treating information as a national asset, determining risk as it applies to information sharing, and using information to support decision making.[54] The Strategy set goals like supporting collaboration and accountability, establishing common standards, improving service and interoperability, improving information security, and protecting civil rights and privacy.[55] This policy established the most current goals concerning information sharing but does nothing to endorse or recommend a method for accomplishing those goals.

A 2012 GAO report titled, *Key Considerations for Implementing Interagency Collaborative Mechanisms*, outlined a series of planning considerations that contribute to successful collaboration: establishing outcomes and accountability, bridging across organizational cultures, sustaining leadership, clarifying roles and responsibilities, including all relevant participants, and providing sufficient resources and written guidance and agreements that support continuity.[56] These contributions served as a guide provided by the GAO to organizations to begin broad improvements to information sharing. This quality was missing from previous legislation and policy. These considerations can also inform the development of rules to guide the development and sustainment of an ESN.

Another GAO report from 2012 titled, *Information-sharing-DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and*

---

[53] White House, *National Strategy for Information-sharing and Safeguarding*, 1.

[54] Ibid., 6–7.

[55] Ibid., 8–13.

[56] Christopher J. Mihm, *Key Considerations for Implementing Interagency Collaborative Mechanisms* (GAO-12-1022) (Washington, DC: Government Accountability Office, 2012), http://www.gao.gov/assets/650/648934.pdf.

*Strengthen Efforts*, was a comprehensive look at the DHS's entire approach to information sharing.[57]

The Report identified three significant findings contributing to the DHS' information-sharing challenges. First, no process is in place to document information-sharing gaps across the agency. Second, no process has been implemented to determine the causes of gaps once identified. Third, no process exists for identifying and assessing the impacts of reprioritizing initiatives should they prove ineffective.[58] Fundamentally, the DHS is experiencing the same challenges facing the rest of the HSE and has been unable to answer those challenges effectively.

On June 2014, the DHS published the *Quadrennial Homeland Security Review* (QHSR) to provide a comprehensive look into the priorities for the DHS and the HSE.[59] Three watershed events mentioned in the opening of the review are the Deepwater Horizon oil spill, Hurricane Sandy, and the Boston marathon bombing.[60] The DHS has a broad mission space and the QHSR lists terrorism prevention and security enhancement as the cornerstone.[61] Other mission areas include securing and managing the borders, enforcing and administering immigration law, safeguarding and securing cyberspace, and strengthening national preparedness and resilience.[62] All these mission areas have information-sharing components operating at different levels of effectiveness. Without significant improvement in information-sharing efforts, it is unclear how the DHS can be successful in these mission areas.

---

[57] Eileen Larence, *Information-Sharing—DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts* (GAO-12-809) (Washington, DC: U.S. Government Accountability Office, 2012). http://www.gao.gov/assets/650/648475.pdf.

[58] Ibid., 29–30.

[59] U.S. Department of Homeland Security, *2014 Quadrennial Homeland Security Review* (Washington, DC: U.S. Department of Homeland Security, 2014), http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

[60] Ibid., 5.

[61] Ibid., 14.

[62] Ibid.

The DHS listed activities and actions that drive activity in those mission areas. Those drivers are the evolution of the terrorist threat, the use of information and communications technology, natural disasters to include pandemics and climate change, interdependent and aging critical infrastructure systems and networks, the increasing volume and speed of the flow of peoples and goods, and budgetary constraints.[63] It would seem the DHS would benefit from a low cost, scalable, decentralized, and stable information-sharing platform that supports collaboration between the public and private sectors.

The Review referred to threats as "strategic challenges." They are evolving terrorist capability, cybersecurity threats to infrastructure, biological concerns to include bioterrorism, pandemics and animal diseases, the use of an improvised nuclear device, transnational criminal organizations, and large-scale natural hazards.[64] These parallel the threats found in the Worldwide Threat Assessment.

The QHSR then outlined the guiding principles as they apply to those threats. The cornerstone of HS is the multi threat and all hazard prevention of terrorism followed by supporting economic security, maintaining a networked community, using market-driven solutions, while preserving of privacy, civil rights and civil liberties, and seeing HS as national risk management.[65] These same principles apply to effective information sharing.

The Review made a few significant points while illustrating what the future of HS would look like. The first is that the world is becoming more connected and the speed at which information moves is increasing. An infographic in the Review shows two billion users on 12 billion devices in 2012 and that number is expected to double by 2017.[66] Thus, web-based information sharing appears to be a very prudent means of collaboration.

---

[63] U.S. Department of Homeland Security, *2014 Quadrennial Homeland Security Review,* 14.

[64] Ibid., 28.

[65] Ibid., 30–32.

[66] Ibid., 20.

The Review stated suspicious activity reporting (SAR) is a DHS priority and is an information-driven activity.[67] The QHSR also made an important point about information quality by stating information needs to be timely, relevant, accurate, and trusted.[68] This statement reflects the goal of the *National Strategy for Information-sharing and Safeguarding* and illustrates the continuing need for an effective information-sharing platform to support the HSE.

The DNI issued his *Strategic Vision for 2015* and emphasized continued collaboration within the IC with a focus on agency and functional boundaries, giving assets more autonomy, giving customers greater access to information to allow them to tailor requests to their needs, and improving collaboration across the intelligence enterprise.[69] This report is another policy document supporting increased collaboration without providing a framework to achieve that goal when a web-based decentralized platform designed to support collaboration would be an appropriate approach.

A CRS report titled, *Legislation to Facilitate Cybersecurity Information-sharing: Economic Analysis*, from December 2014, discussed using legislation to drive cybersecurity information sharing and highlighted challenges and issues facing this effort. The report asserted experts in the cybersecurity field feel the need for improved information sharing among individuals, companies, non-governmental organizations, and governments is essential to improving security.[70] The report also covered the varieties of information that can be shared to include ways of detecting specific attacks, general information about hardware, software, and procedures, as well as information about recovering from breaches of data. The report emphasized the cost of information sharing is small while the benefits can be large.[71] This report is the first of its kind to apply a type of cost-benefit model to information sharing.

---

[67] U.S. Department of Homeland Security, *2014 Quadrennial Homeland Security Review*, 38.

[68] Ibid., 51.

[69] James McConnel, *Director of National Intelligence Strategic Vision 2015* (Maxwell AFB, AL: The Air University, 2014), http://www.au.af.mil/au/awc/awcgate/dni/vision_2015_july08.pdf.

[70] N. Eric Weiss, *Legislation to Facilitate Cybersecurity Information-sharing: Economic Analysis* (CRS Report No. R43821) (Washington, DC: Congressional Research Service, 2014), 2, http://www.fas.org/sgp/crs/misc/R43821.pdf.

[71] Ibid., 2.

CRS asserted it is beneficial for firms to share information broadly. In doing so, they are supporting firms that may not have the resources to protect themselves or inform consultants to develop protective measures. One firm or organization tends to the one paying for this development, which is the challenge with this approach. Another concern is the bad publicity a breach can have on a firm's profitability.[72] This report deals specifically with cybersecurity but the findings apply across the HSE. The burden to create a solution born by one participant is not always shared by those benefiting from the result. While also myopic, it is a challenge of decentralized collaboration. Over time, every participant contributes and benefits to generally the same degree.

The report suggested information sharing as a relatively inexpensive approach for a group of companies to improve their cybersecurity.[73] The report also asserted firms and industry groups are hesitant to share information for fear they might violate privacy or antitrust laws or release proprietary information.[74] Ultimately, the benefits of information sharing are difficult to measure or quantify while the risks are clear.[75] The current information-sharing construct does not provide enough incentive to make it worthwhile for the private sector to participate. Incentives for participation in information-sharing platforms are essential to success. Recognition for excellence in sharing needs to be as highly regarded as what is done with the shared information.

CRS illustrated the waste created by not sharing information results in duplicative effort. When information is shared, the savings created by eliminating duplicative effort creates additional resources that can then be applied to improving cybersecurity.[76] The report then discussed the challenge of assessing security product effectiveness. It is difficult to discern if a product is good or the opponent lacks competence, but in either case, the value of the product typically cannot be determined.[77] It can be frustrating,

[72] Weiss, *Legislation to Facilitate Cybersecurity Information-sharing: Economic Analysis*, 3.

[73] Ibid.

[74] Ibid., 4.

[75] Ibid., 5.

[76] Ibid., 11.

[77] Ibid., 12.

especially for the private sector, to waste limited resources on ineffective security products. Using an ESN approach could help eliminate that waste.

This report is the most comprehensive review of the challenges of information sharing as a discipline even though it is set against the backdrop of cybersecurity. The findings in this report apply across the HSE and can be addressed by an ESN supported by the federal government.

The most recent *National Security Strategy* was published in February 2015. The term "information-sharing" is only mentioned twice in the 35-page document.[78] The 2010 *National Security Strategy* mentioned the term four times and an entire section was devoted to information sharing.[79] This approach appears to be a shift away from making information sharing a priority instead to merely acknowledging its existence. The Strategy emphasized global leadership with a focus on defeating the Islamic State of Iraq and the Levant (ISIL), opposing Russian acts of aggression, stopping the expansion of violent extremism in Africa and Europe, supporting cybersecurity, and leveraging the energy revolution.[80] These areas will all require collaboration across a wide variety or both public and private organizations. It seems to be a puzzling policy trend that as a collaborative information-sharing platform becomes a more obvious answer to significant policy challenges, the less policy support it receives.

EO 13691, titled *Promoting Private Sector Cybersecurity Information-sharing*, was published in February 2015. It addressed improving general cybersecurity through information sharing to assist both public and private organizations involved in public health and safety, national security, and economic security.[81] The EO established

---

[78] White House, *2015 National Security Strategy* (Washington, DC: White House, 2015), http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

[79] White House, *2010 National Security Strategy* (Washington, DC: White House, 2010), http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[80] White House, *2015 National Security Strategy*.

[81] "Executive Order -- Promoting Private Sector Cybersecurity Information-sharing," February 13, 2015, http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing.

information-sharing and analysis organizations (ISAOs) to serve as the coordinating and collaborative entities for cyber security across the public and private sectors.[82]

The DHS is the designated federal lead in this effort and the National Cybersecurity and Communication Integration Center (NCCIC) is the focal point for inclusion, collaboration, and coordination among the ISAOs.[83] The EO did not provide a formal structure for the ISAOs to allow them to grow as the users see fit and adapt as necessary. It seems like an excellent opportunity to create an ESN to meet this policy directive, as well as others previously mentioned.

## C. COLLECTIVE INTELLIGENCE

No discussion of collaborative creation would be complete without elaborating on the concept of collective intelligence. The Massachusetts Institute of Technology (MIT) cites Pierre Levy as the first to conceive of the concept of collective intelligence. It is defined as, "a form of universally distributed intelligence, constantly enhanced, coordinated in real time and resulting in the effective mobilization of skills."[84] It is plain to see how this concept is applicable to unifying the HSE by creating a BoK. The next section explores this concept.

The multidisciplinary nature of the HS discipline paired with the wide variety of participants in the HSE lends itself to the collaborative capabilities of collective intelligence. Taking a bottom-up approach to establishing a BoK is found to be the best approach according to Yoshifumi Masunaga and his colleagues in their work, *A Wiki-based Collective Intelligence Approach to Formulate a Body of Knowledge (BOK) for a New Discipline*.[85] This approach is especially applicable to HS in the absence of a singular understanding of the discipline.[86]

---

[82] "Executive Order -- Promoting Private Sector Cybersecurity Information-sharing."

[83] Ibid.

[84] Daren C. Brabham, *Crowdsourcing* (Cambridge, MA: The MIT Press, 2013), locations 424–428, Kindle edition.

[85] Yoshifumi Masunaga, Yoshiyuki Shoji, and Kazunari Ito, "A Wiki-based Collective Intelligence Approach to Formulate a Body of Knowledge (BOK) for a New Discipline," in *Proceedings of the 6th International Symposium on Wikis and Open Collaboration*, art. 11. Gdansk, Poland—July 07–09, 2010 (New York: ACM, 2010), 3.

[86] Ibid.

James Surowiecki studied collective intelligence extensively in his bestselling work, *The Wisdom of Crowds.* He establishes key points in support of collective intelligence. The human being is designed to work collectively. For example, "With most things, the average is mediocrity. With decision-making, it's often excellence. You could say it's as if we've been programmed to be collectively smart."[87] He also establishes the three conditions needed to be effective collectively: "diversity, independence, and decentralization."[88]

Regardless of singular expertise, pooled expertise is more effective and reliable as proposed by Surowiecki. "The larger the group, the more reliable its judgment will be."[89] He also emphasizes the need for a smart group, "Trying to find smart people will not lead you astray. Trying to find the smartest person will."[90] Once a smart group has formed, it needs to specialize. Specialization increases productivity and efficiency, as well as increasing the scope and the diversity of the opinions and information in the system.[91]

Surowiecki has established the strengths and weaknesses of collective intelligence as well. The strengths are based on independence and specialization while allowing for coordinated activities and solving difficult problems. The main weakness is the lack of a guarantee that information of value will circulate through the system.[92] He also cautions against centralization in the structure of the system and encourages the value of aggregation.[93]

Surowiecki cites other scientists who support the power and effectiveness of collaboration. Economist Paula Stephan has argued, "Scientists who collaborate with each other are more productive, often times producing 'better' science, than are individual investigators." In addition, social scientist Etienne Wenger adds, "Today's

---

[87] James Surowiecki, *The Wisdom of Crowds* (New York: Knopf Doubleday Publishing Group, 2005), 9, Kindle edition.

[88] Ibid., 20.

[89] Ibid., 32.

[90] Ibid., 34.

[91] Ibid., 69.

[92] Ibid.

[93] Ibid., 76.

complex problem solving requires multiple perspectives. The days of Leonardo da Vinci are over."[94] He then illustrates that collective intelligence goes beyond simple collaboration, which is cumulative. Collective intelligence is simultaneous. Collective intelligence is interdependent.[95]

Ori Brafman and Rod Beckstrom establish an important principle of centralization in their book, *The Starfish and the Spider*, which states, "an open system doesn't have central intelligence; the intelligence is spread throughout the system. Information and knowledge naturally filter in at the edges, closer to where the action is."[96]

The study of collective intelligence is from a variety of methods to include theoretical, conceptual, simulations, case studies, experiments, and systems design.[97] It is also a multidisciplinary field involving psychology, complexity, cognition, biology, computer science, and communication.[98] With so many methods and fields involved, no single, "theory capable of explaining how collective intelligence actually works"[99] exists.

## D. CROWDSOURCING

A similar concept to collective intelligence is crowdsourcing, which takes the shared knowledge of a group and puts it into action. The MIT Center for Collective Intelligence published a comprehensive review of crowdsourcing. In it, crowdsourcing is defined as, "a phenomenon where groups of people working together or taken in the aggregate become collectively intelligent as an entity."[100] The next section explores the literature that explains this phenomenon.

Many organizations, to include government agencies, regularly use online communities to accomplish a variety of creative tasks. The most effective arrangement is

---

[94] Surowiecki, *The Wisdom of Crowds*, 160.

[95] Ibid., 162.

[96] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (London: Penguin Group USA, 2006), 39–40, Kindle edition.

[97] Juho Salminen, *Collective Intelligence in Humans: A Literature Review* (Ithaca, NY: Cornell University Library, 2012), 1, https://arxiv.org/abs/1204.3401.

[98] Ibid.

[99] Ibid.

[100] Brabham, *Crowdsourcing*, Kindle locations 1387–1389.

for bottom-up efforts to be driven by established top-down organizational goals, the root of crowdsourcing.[101] Crowds must satisfy four conditions to be considered "wise." Those conditions are a diversity of opinion, independence, decentralization, and aggregation.[102]

While many think crowdsourcing is what happens when a large group does anything, Daren Brabham defines crowdsourcing as, "an online, distributed problem-solving and production model that leverages the collective intelligence of online communities to serve specific organizational goals."[103] Brabham also establishes the key ingredients of crowdsourcing as, "an organization that has a task it needs performed, a community (crowd) that is willing to perform the task voluntarily, an online environment that allows the work to take place and the community to interact with the organization, and mutual benefit for the organization and the community."[104]

"Conceptually, crowdsourcing can be explained through the processes of problem solving and innovation as well as through the group phenomena of collective intelligence and the wisdom of crowds."[105]

The maturity of a discipline determines how its BoK is formulated. A mature discipline, like computer science, can assemble its BoK with a small group using a top-down approach because the majority of the participants have a comprehensive knowledge of the discipline. An immature discipline, like HS, is best suited to a bottom-up approach because the majority of the participants do not have that comprehensive knowledge.[106] Masunaga makes this powerful yet simple assertion, "In general, a discipline is defined on the basis of its BoK."[107]

---

[101] Brabham, *Crowdsourcing*, Kindle locations 106–109.

[102] Surowiecki, *The Wisdom of Crowds*, 8.

[103] Brabham, *Crowdsourcing*, Kindle locations, 138–141.

[104] Ibid., 222–227.

[105] Ibid., 299–300.

[106] Masunaga, Shoji, and Ito, "A Wiki-based Collective Intelligence Approach to Formulate a Body of Knowledge (BOK) for a New Discipline," 1.

[107] Ibid.

A BoK is a restricted version of a semantic network. A wiki-based BoK provides "an environment for participants in a specific discipline to assemble a BoK for that discipline which can be represented by a conceptual tree."[108] The construction of a BoK from the bottom up requires the analysis of available materials to establish a level of knowledge.[109]

Contributors in a participatory culture are motivated to provide content in an ESN when they perceive their peers are finding value in their contribution, namely through comments and other feedback.[110]

## E. ENTERPRISE SOCIAL NETWORKS

An ESN is a, "collection of tools and processes that support social interaction within any type of private or public organization."[111] These tools can be described separately by applications to include wikis and blogs or could be interpreted to include a more integrated approach using an existing platform like Facebook or Twitter.[112] The next section explains the purpose and function of this powerful collaboration tool.

A primary purpose of an ESN is to connect existing teams across an enterprise to break down pockets of information and then create a place or community where that information can be shared in a more organized and deliberate fashion. As opposed to well defined and task organized teams with specific membership, communities are more flexible and adaptive with the expectation that they and the topics they are involved in will evolve over time.[113]

---

[108] Masunaga, Shoji, and Ito, "A Wiki-based Collective Intelligence Approach to Formulate a Body of Knowledge (BOK) for a New Discipline," 3.

[109] Ibid.

[110] Brabham, *Crowdsourcing*, Kindle locations 848–852.

[111] Frank Leistner, *Connecting Organizational Silos: Taking Knowledge Flow Management to the Next Level with Social Media* (Hoboken, NJ: Wiley, 2012), 2, Kindle edition.

[112] Ibid.

[113] Ibid., 9–10.

ESNs streamline knowledge flow when an enterprise adopts and fosters a "need to share" approach by making it easy for anyone to participate. This approach is especially true when applied to those contributors that might otherwise be hesitant to share in a highly structured and hierarchical knowledge sharing effort.[114] This approach is also extraordinarily efficient when working in such an amorphous enterprise as HS.

The most valuable aspect of an ESN is its ability to reduce blockages of information flow. Typical blocks that can be addressed include missing trust, lack of connectivity, geographic, political or cognitive borders, situational awareness across diverse communities, and general resistance to new ideas from outside the team.[115]

Of significant importance to the success of an ESN is the vigorous support of a driving team providing sustained strategic and operational guidance to keep the users engaged and motivated. The technology alone will not sustain the enthusiasm necessary for a truly successful ESN. It will need substantial marketing activities to keep the benefits and advantages in the spotlight.[116] The team will also be crucial in not only addressing problems and concerns but collaborating with the users to achieve a consensual outcome.

Training will be a key component to the success of the ESN as well. This training goes beyond the simple technical use of the platform. All users will need to understand their roles and responsibilities in producing and consuming contributions.[117]

Companies have been using social media and Web 2.0 tools to include blogs and wikis since 2005. A well-established key to success is top-down support of employees using the platforms and accepting the time it takes to become competent in its use. Once this hurdle is cleared, the majority of organizations and their senior leadership acknowledge the potential and encourage the usage of the ESN.[118]

---

[114] Leistner, *Connecting Organizational Silos: Taking Knowledge Flow Management to the Next Level with Social Media*, 11.

[115] Ibid.

[116] Ibid.

[117] Ibid.

[118] Ibid., 12.

Some key participants in successful ESNs are early adopters who get in on the ground floor and help spread awareness and illustrate benefits. Evangelizers may not be users but are influencers within the organization and can increase the participation of others. Then drivers are those who sweep through an organization to pick up those resistant to participation.[119]

The cultural implications of an organization adopting an ESN are significant. A lot of trust is required from management and employees to do the right things to sustain the network. That trust can have a significant impact on the effectiveness and efficiency of an organization.[120]

The external affairs components of an organization are a good place to look for early adopters because they are comfortable with the technology and understand the connective power of the platform. They are useful in translating that capability and power internally and then bridging the gap between the internal and external networks.[121]

An ESN is an infrastructure for connection, and as such, can break down the obstacles in the knowledge flow by serving as a "super water cooler" for collaboration; with that being said, it should not be expected that "every employee is connected to every other employee and they are all engaged in active discussions."[122] ESNs do not replace normal interaction as much it enhances the ability of an organization, especially a disbursed one, to collaborate and share knowledge more effectively and efficiently.

Expect a significant challenge from employees who are most comfortable with email (a "need to know" information-sharing platform) and inexperienced with social media and yet judge it ineffective.[123] This obstacle can be cleared through training, marketing, and integration of the ESN into the everyday operations of the enterprise.

---

[119] Leistner, *Connecting Organizational Silos: Taking Knowledge Flow Management to the Next Level with Social Media*, 45.

[120] Ibid., 16–18.

[121] Ibid., 20.

[122] Ibid., 31.

[123] Ibid., 31–32.

A management advantage to an ESN is the visibility it provides into the connectedness of the organization. Leadership can see who is connected to whom and how often they communicate. It also builds resiliency and continuity within the organization by maintaining linkages regardless of geographic or organizational movement individually or as a group.[124]

An ESN has the ability of allowing the network to critique new ideas and address weaknesses or incompleteness before resources are unnecessarily spent. It is essentially an instant reality check.[125]

ESNs work to reduce personal and technical isolation. When employees receive more input, they learn more, which increases morale and motivation. This concept is more magnified when they have connections to experts and their associated expertise at a personal level, which considerably contributes to increased efficiency and bridged silos.[126]

## F. WIKIS

A wiki is the confluence of collective intelligence and crowdsourcing where people possessing parts of a greater knowledge can effectively "meet" to create a knowledge product like a BoK. The next section explains what a wiki is and what it can do.

Ward Cunningham is considered the father of the Wiki concept and all things Wiki.[127] A wiki is technically considered a discussion and collaboration server used as a tool to collect and cross reference information.[128] Cunningham refers to a wiki as, "the simplest database that could possibly work."[129] What makes a wiki a unique group communication mechanism is the ability for, "the organization of contributions to be

---

[124] Leistner, *Connecting Organizational Silos: Taking Knowledge Flow Management to the Next Level with Social Media*, 33.

[125] Ibid., 35.

[126] Ibid., 27.

[127] Bo Leuf and Ward Cunningham, *The Wiki Way: Quick Collaboration on the Web* (Boston, MA: Addison-Wesley Professional, 2001), xix.

[128] Leuf and Cunningham, *The Wiki Way: Quick Collaboration on the Web*, 3.

[129] Ibid., 15.

edited in addition to the content itself."[130] Open editing allows non-technical users to create and edit web content, which is a powerful effect of a wiki's usage.[131] The potential and reach of a wiki is unlike anything used to this point.

"A wiki invites all users to edit any page or to create new pages within the wiki website, using only a plain vanilla web browser without any extra add-ons," "wiki promotes meaningful topic associations between different pages by making page link creation almost intuitively easy and by showing whether an intended target page exists or not," and "a wiki seeks to involve the visitor in an ongoing process of creation and collaboration that constantly changes the website landscape," are the fundamental functions of a wiki.[132]

Wikis offer a few functions that differentiate them from other collaborative platforms. The most notable is the Edit button, which is the capability that allows virtually instantaneous collaboration. While not without some difficulties, a competent administrator can establish ground rules and mediate most conflicts. The next function that differentiates wikis is the ability to link articles, which creates a network structure as the wiki becomes more mature. The history function is valuable in that it allows everyone to see how the article has evolved as more information is added and also serves as a safety net should the article need to be "rolled back" to restore content. Wikis usually offer a place to reference instructions and introductions at a homepage referred to as a "sandbox." Lastly, most wikis have a simple search function that relies on a well-thought titling system to serve as an indexing system.[133]

Ultimately, it is important to understand any wiki relies on key components of large group dynamics. The first is playful creation or a "loose, playful atmosphere and fun at work" that makes wikis "cool." The next component is a flat hierarchy necessary for decisive creative and self-organized group processes by distributing both the risks and advantages followed by the group need to modify complex topics regularly that challenge

---

[130] Leuf and Cunningham, *The Wiki Way: Quick Collaboration on the Web*, 15.

[131] Ibid.

[132] Ibid., 16.

[133] Anja Ebersbach et al., *Wiki: Web Collaboration* (Berlin: Springer Science & Business Media, 2008), 19–20.

contributors to avoid unnecessary contributions as those articles are ignored. The simplicity of the system and the rules help to overcome the greatest obstacle of a wiki, which is making the decision to join in the effort. The openness and mutual trust of a wiki is also important despite inevitable conflicts.[134]

An essential consideration when establishing a wiki is an awareness of the potential problems a wiki will face. The first and most significant is a lack of interest. If a wiki is not acknowledged as a tool and made part of a daily routine, it will stagnate and lose relevance. The "freshness" of the information is vital and is maintained through regular contribution. The key to success is buy-in at the highest level by accepting open participation. Conversely, mandatory participation is as damaging as not participating because quality falls off and user benefit is lost.[135]

Another challenge facing many wikis is conflict management. Just like the physical world, inevitably some participants will be interested in their own self-promotion or will tear down others with differing perspectives. The key to successfully managing this challenge is a clear and effective community portal page where "guidelines and conventions, discussion pages for admin candidates, moderation information and pages collecting opinion statistics," as well as completed problem cases are listed on arbitration pages.[136]

## G. KEY FINDINGS

The review of the literature related to information-sharing legislation and policy followed by critiques of that legislation and policy has revealed the following findings.

- Legislation and policy place significant pressure on sharing information in virtually all directions and yet does not provide much in the way of guidance or measures to support that direction.
- An information-sharing policy loop has developed that wastes resources and fails to achieve effectiveness. A policy loop occurs when issues and recommendations feed into each other without the goal of a solution or a process to resolve the issue.

---

[134] Ebersbach et al., *Wiki: Web Collaboration*, 22–23.

[135] Ibid., 26–27.

[136] Ibid., 29.

- Legislative direction is out of date and information sharing is losing momentum as a priority in the HS scheme.

To add to the challenge, the last piece of significant information-sharing legislation was passed in 2007. These conditions resulted in many organizations creating their own information-sharing platforms to meet their individual needs, which resulted in a disunity of platforms, duplicity of effort, and additional wasted resources. Worst of all, information was still not being shared effectively with those who needed it; the commonly agreed upon goal of any information-sharing effort.

- Private ESN platforms are growing participants and improving capabilities while the HSE has not yet been able to develop an efficient platform for broad dissemination of simple, unclassified, but timely information.

Cultural challenges also arose, as policymakers had to shift away from the philosophy of "need to know" to one of "need to share." This approach still has not been effectively implemented by any organization or platform. Protecting privacy and civil rights and maintaining security adds additional complexity to an already complex problem. Add to that the need to share information with organizations like state, local, tribal, and territorial (SLTT) governments and the private sector, and the problem becomes very daunting.

It is possible that this frustrating situation could cause apathy and fatigue for legislators and the rest of the information-sharing community that could result in the defunding of and disinterest in further information-sharing efforts and a return to the pre-information-sharing era. Simply put, a single platform does not exist from which all HSE partners can securely receive vetted general information and collaborate with a wide variety of mission partners. While appearing simplistic, simplicity in information sharing however is a benefit. The ubiquity of a platform like Wikipedia is proof of this concept.

Very little discussion has taken place in advancing information sharing beyond the current state. It might be expected that a more comprehensive plan to keep pace with technological advances in information sharing would be advanced. The topic of virtual collaboration has also received scant attention. At some point, information sharing should move beyond simply moving information from one place to another and focus on collaboration.

- Collective intelligence and crowdsourcing are a proven method of creating a BoK and the HSE does not currently have a BoK.

The HSE is a discipline and a mature discipline significantly benefits from a BoK. The development of a HSE BoK is vital to growth and the perpetuation of the discipline. The defuse nature of the HSE makes crowdsourcing, specifically a wiki, an applicable approach to creating and sustaining the HS BoK.

A reasonable concern is how can another information-sharing platform be assured to meet these shifting requirements? The next chapter proposes rules that could be applied to all ESNs and a rubric that can be used to determine the maturity of an ESN and provide guidance for advancing maturity to a mastery level.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. THE RULES AND A RUBRIC

To this point, this thesis has established that the demand for information sharing across the HSE persists despite the absence of clear direction. It has also been asserted that established platforms are available that attempt to answer this demand and yet they all are too isolated to reach across the whole HSE in any useful manner, which has resulted in a stale "transmit only" approach.

A collaborative effort in information sharing has been in place outside of the HSE for over a decade and has been growing in size and credibility. If the HSE intends to be considered a legitimate discipline, it will need to develop a BoK. Leveraging the entire HSE to do so in a collaborative fashion will dramatically accelerate the development of the BoK and improve the accuracy and currency as well.

A reasonable concern would be how this process could be managed to provide some confidence that this approach will not meet the same fate as previous efforts. This chapter proposes and discusses some simple rules and a rubric that could improve the cultural development of a knowledge sharing ESN. Current rules associated with a HSE-related information-sharing platform deal more with program management concerns with very little guidance related to collaboration.

The Merriam Webster dictionary offers three definitions of the noun *rule*. The first is, "a statement that tells you what is or is not allowed in a particular game, situation, etc." The second is, "a statement that tells you what is allowed or what will happen within a particular system (such as a language or science)." The third is, "a piece of advice about the best way to do something."[137] This thesis utilizes the third version. The rules referenced in this paper are intended to serve as thorough guides and not as absolutes. It would be foolish to impart a legislative tone to a system that needs to be self-assessive and rapidly adaptive.

[137] *Merriam-Webster Dictionary*, s.v. "Rule," accessed October 2, 2016, http://www.merriam-webster.com/dictionary/rule.

Rules like the ones about to be proposed do not currently exist within the HSE because no structure currently exists in which to apply them. These rules are intended to increase the level of comfort of the HSE to prompt the acceptance of an ESN, and ultimately, the establishment and maintenance of a HSE BoK to serve the broad spectrum of the HSE.

## A. DEVELOPMENT OF THE RULES

In February 2000, Hans-George Gruber and Dr. Linda Duxbury wrote "Does Organizational Culture Affect the Sharing of Knowledge?" It is a thesis that studies information sharing within a high tech company. In it, Gruber and Duxbury propose five topic areas discussed in the conclusion: openness, trust, communication, top management support, and reward structure.[138] These topic areas are the basis for the soon to be proposed rules. They represent cultural components that directly impact participation in any community, virtual or real.

The concept of openness refers to the environment supporting knowledge sharing and focuses on a shared objective with minimal ulterior motives. Gruber and Duxbury assert this component is critical to information sharing.[139]

Trust applies to the actual exchange of information. Trust is the propellant to knowledge sharing when tied to mutual respect and shared objectives.[140] This consideration will be important when developing a vetting methodology in the creation of a HSE ESN. Answering the question of who can share what information with whom is a well-established challenge.

The ability to communicate clearly and across a variety of topics is essential to knowledge development. The quality and diversity of communication contributes directly to knowledge exchange and combination.[141] An important recommendation related to communication is to diversify communication despite what might be the primary means.

---

[138] Hans-Georg Gruber, "Does Organizational Culture Affect the Sharing of Knowledge, The Case of a Department in a High Technology Company" (master's thesis, Carleton University, 2000), 189–193.

[139] Ibid., 190.

[140] Ibid.

[141] Ibid., 191.

Seminars and mentoring programs are vital means of communication even if the organization is primarily a virtual community.[142]

Gruber and Duxbury found active participation and support from senior leadership is also a key component of knowledge sharing. An information-sharing platform simply will not be successful unless it is an integral part of the organization's communication scheme, which is driven by senior leadership. If senior leaders are not regularly seen on the platform, it will struggle for relevance.[143]

Positive reinforcement keeps participants coming back to the sharing platform. A varied reward system needs to involve peer recognition and incentives from senior leadership.[144] Success cannot be guaranteed without a reward system and the appropriate behavior to reward must be carefully considered.[145] Rewarding the wrong behavior can lead to wasted resources and damages the legitimacy of the platform through rewarding the wrong participants for the wrong reasons.

Kamiz Dalkir, in his second edition of *Knowledge Management in Theory and Practice*, cite and then expand upon Gruber and Duxbury's work by providing their interpretation of the best practices for knowledge sharing. They propose an emphasis on virtual organizations, support for participants, multidirectional information flow, trust, shared objectives, development and evolution over time, and creation of a permanent organizational memory.[146]

Ultimately, both bodies of research agree on six topic areas: the necessary involvement of senior leadership, participants' mutual interaction, the importance of connecting people to gather content, acceptance of cultural change over time, the value of role models, and reliable and regular communication. These topic areas have been refined to constitute the six rules proposed in this thesis.

---

[142] Gruber, "Does Organizational Culture Affect the Sharing of Knowledge, The Case of a Department in a High Technology Company," 191.

[143] Ibid., 192.

[144] Ibid.

[145] Ibid.

[146] Kimiz Dalkir and Jay Liebowitz, *Knowledge Management in Theory and Practice* (Cambridge, MA: The MIT Press, 2011), Kindle locations 3029–3032, Kindle edition.

## B. THE RULES

The aggregated rules proposed by this thesis are the following.

- Rule One—Allow cultural change over time
- Rule Two—Create opportunities for people to get to know one another
- Rule Three—Focus on connecting people over gathering content
- Rule Four—Top-down support of bottom-up solutions
- Rule Five—Provide positive role models wherever possible
- Rule Six—Consistently reward knowledge-sharing behavior

These rules require some explanation to provide an adequate context for the rules themselves and to support the rubric supporting the implementation of the rules. Rule One reinforces the simple idea that any collaborative community has no choice but to evolve over time. Processes will be refined and normative behavior will require necessary changes to minimize bias and increase the rigor of the community.

Rule Two emphasizes the importance of the degree of connectedness among the participants in the community. One way to think of it is to rewrite the idea of the concept cited in the 9/11 Report of "connecting the dots" where the dots are assumed to be pieces of information. Instead, this rule asserts the "dots" are actually people and that the more connected the people are the less likely simple substantive information will fall through the cracks.

Rule Three looks to shift away from the old paradigm of "need to know" towards a more substantial one of "need to share." While not a new concept, it has proven difficult to implement because the focus typically is on what information is being shared vice who is sharing what information with whom. It is not enough simply to share random pieces of information. People within the community need to know one another, trust one another, and interact on a reasonably regular interval so that timely information is provided in an actionable timeframe.

Rule Four basically speaks truth to power. If legislators and policymakers want improved information sharing, they need to participate in the process actively. HSE senior leadership like the DNI, the Secretary of Homeland Security, the Director of the

Federal Bureau of Investigation (FBI) and their staffs, for example, need to interact regularly with community participants. Members of the Senate and House HS committees need to interact regularly with community participants. Most importantly, these senior leaders need to reach out to the other community participants to remain current on evolving issues. Military commanders refer to this practice as "ground truth."

Rule Five makes the important assertion that regular mentorship and guided discussion need to occur as this process evolves. Expertise in subject matter areas and community processes needs to identified and supported to provide guidance to new participants and update regular users on best practices. This approach is vital to the sustainment of the community, as it establishes continuity and motivates those most active users to share their experiences.

Rule Six is simply the formalization of positive reinforcement. If community participants are performing well, they need to be rewarded for their preferred behavior. Other members will emulate those rewarded behaviors to receive similar rewards. As a result, that practice will grow the use of best practices and the absence of rewards will similarly limit undesirable behavior.

The mere existence of rules does not enable them to be implemented. A rule-based process needs a guide to improve implementation and a rubric is a viable option to serve as that guide. A rubric for the purpose of this thesis is defined as a guide listing specific criteria for scoring. This definition is an adaptation of a few definitions to meet the need of this thesis. A rubric has been developed to assess the maturity of an organization implementing the rules. This rubric can be used to assess an organization to determine initial maturity or it can be used to guide growth as resources and time permit.

## C. A RUBRIC

Concepts for the construction of this rubric were derived from a variety of sources. A significant contributor was the Center on Standards and Assessment Implementation (CSAI) and their series of videos and websites on assessment design. They establish five elements of assessment design; *standardization* or alignment to a set of rules, *rigorousness* or robust measurement of subject capability and measured intent,

*precision* or accurate measurement of knowledge and skills, *impartiality* or avoidance of personal characteristics, and *strategic scoring* or evaluation with a focus on long-term and high-level organizational growth.[147] The proposed rubric needs to meet these five elements.

CSAI outlines the purposes of an assessment as well: diagnostic—a pretest to determine knowledge and skills, formative—to monitor subject behavior, summative—to measure mastery of a standard and interim—to measure against specific criteria like skills, goals, or a timeframe.[148] The purpose of this rubric is summative, as it will assess the mastery of a subject to a predetermined set of standards also known as the rules.

These elements were included in the design of the rubric with the ultimate goal being a rubric that was accurate and consistent. See Table 1.

[147] "Assessment Design Toolkit," accessed October 17, 2016, http://www.csai-online.org/spotlight/assessment-design-toolkit#repurpose the toolkit.

[148] "Part 1—Key Concepts," accessed October 17, 2016, http://www.csai-online.org/spotlight/part-i-key-concepts#part-2.

Table 1. The Rubic.[149]

| The Enterprise Social Network Assessment Rubric | | | | | | |
|---|---|---|---|---|---|---|
| Purpose: Assess the degree of compliance to the openness rules. (Summative) | | | | | | |
| | Emerging | | Developing | | Mastering | |
| ***The Rules*** | **1 Point - Remembering** | **2 Points - Understanding** | **4 Points - Analyzing** | **3 Points - Applying** | **5 Points - Evaluating** | **6 points - Creating** |
| 1. Allow cultural change over time. | Choose an adaptive culture. | Define what culture change means to the ESN. | Examine the pace of culture adaptation. | Build a process to support culture change. | Prioritize the need to have an adaptive culture. | Design cultural adaptation into the ESN. |
| 2. Create opportunities for people to get to know one another. | Recognize the value of networking. | Illustrate opportunities for networking. | Categorize the degree of connectedness. | Develop a plan for networking. | Defend innovative networking. | Develop methods to improve networking. |
| 3. Focus on connecting people vice capturing content. | Identify the difference between connecting people and capturing content. | Explain the difference between connecting people vice capturing content. | Attribute value to connecting people. | Demonstrate the defense between connecting people vice capturing content. | Assess the quality of interpersonal connections. | Validate interpersonal connections. |
| 4. Top-down support of bottom-up solutions. | Define solution support. | Illustrate the benefit of top-down support to bottom-up solutions. | Simplify the communication process for solution support. | Develop a process to streamline solution support. | Support the process of top-down support to bottom-up solutions. | Integrate leadership into bottom-up problem solving. |
| 5. Provide positive role models wherever possible. | Select personnel to serve as role models. | Explain the responsibilities of a role model. | Examine the duties of a role model. | Demonstrate the responsibilities of a role model. | Prioritize the need for role models in the ESN process. | Develop a sustainability plan for role models. |
| 6. Consistently reward knowledge sharing behavior. | Define knowledge sharing behavior. | Illustrate examples of knowledge sharing behavior. | Examine best practices of knowledge sharing behavior. | Model the best examples of knowledge sharing behavior. | Prioritize the need for knowledge sharing behavior. | Generate a culture of support for knowledge sharing behavior. |

[149] Source: Washington State University, *Guide to Rating Critical & Integrative Thinking Washington, Fall 2006* (Pullman, WA: Washington State University, 2006), http://www.cpcc.edu/learningcollege/learning-outcomes/rubrics/WST_Rubric.pdf.

This rubric satisfies all the elements of standardization, rigorousness, precision, impartiality, and strategic scoring. The use of the already established rules satisfies the element of standardization. Creating a progressive matrix where ESNs are plotted for their current maturity, as well as illustrating a path to improved maturity, addresses the element of rigorousness.

Bloom's Taxonomy was the basis for satisfying the precision element. Ranging the rules along Bloom's taxonomic spectrum (remembering, understanding, applying, analyzing, evaluating, and creating) uses a well-established and accepted cognitive structure. Impartiality is addressed by eliminating any reference to race, gender, or socioeconomics.

An additional layer of rigor is added by showing transitive progression using the Washington State University's rating process by grouping the remembering and understanding components of Bloom's Taxonomy under the term *emerging*, the applying and analyzing components under the term *developing*, and the terms evaluating and creating under the term *mastering*.[150] This structure serves to illustrate phases ESNs can move through as they improve the effectiveness of their knowledge sharing.

Tying the rules to the taxonomic groups are the individual qualities created by combining them into an action. The next section discusses each of the actions tied to each of the taxonomic column and the rule row as shown in the rubric table.

The intent of the rubric is to get an ESN to grow along the rule row and progress from left to right along the taxonomic columns. Obviously, a new ESN does not need to start at the far left. It would be desirable to start as far right as resources will allow and then use the remaining blocks to the right to guide growth as the ESN matures and more resources become available.

The taxonomic progress of Rule One (allow cultural change over time) begins with *choose an adaptive culture* then *define what culture change means to the ESN* under the Emerging group and the Remembering and Understanding columns, respectively. The

[150] Washington State University, *Guide to Rating Critical & Integrative Thinking Washington, Fall 2006.*

Developing group establishes *build a process to support cultural change* and *examine the pace of cultural change* under the Applying and Analyzing columns. The Mastering group represents the most developed end of the spectrum. *Prioritize the need to have an adaptive culture* and *design cultural adaptation into the ESN* represent the Evaluating and Creating columns. The purpose of this progression is to build in adaptability to the culture.

Rule Two (create opportunities for people to get to know one another) emphasizes the need for real interpersonal relationships for an ESN to be truly successful. The Emerging group begins with *recognize the value of networking* and *illustrate opportunities for networking* under the Applying and Analyzing columns, followed by the Developing group and *develop a plan for networking* and *categorize the degree of connectedness* under the Applying and Analyzing columns. The far end of the spectrum under the Mastering group is comprised of *defend innovative networking* and *develop methods to improve networking* under the Evaluating and Creating columns. The interpersonal relationships created through demonstrated effort are essential to the strengthening of a HS-centric ESN, especially if the purpose is to build and maintain a BoK.

Rule Three (focus on connecting people vice capturing content) embraces the idea that the phrase "connect the dots" does not refer to connecting bits of information and instead refers to connecting people. *Identify the difference connecting people and capturing content* and *explain the difference between connecting people vice capturing content* represent the Remembering and Understanding columns in the Emerging Group. The Developing Group is comprised of the Applying and Analyzing columns and *demonstrate the difference between connecting people vice capturing content* and *attribute value to connecting people* describe the desired activities. *Assess the quality of interpersonal connections* and *validate interpersonal connections* represent the Evaluating and Creating columns of the Mastering Group. This explanation illustrates the degrees of involvement in tying "the dots" together.

Rule Four (top-down support of bottom-up solutions) emphasizes the need for leaders to rely on the ESN participants to solve issues within the ESN and then take

action on those solutions. The Emerging Group consists of the Remembering and Understanding columns, and under those columns are *define solution support* and *illustrate the benefit of top-down support to bottom-up solutions.* The Developing Group entails the Applying and Analyzing columns and they contain *develop a process to streamline solution support* and *simplify the communication process for solution support* respectively. The Mastering Group, Evaluating, and Creating columns are *support the process of top-down support to bottom-up solutions* and *Integrate leadership into bottom-up problem solving.* This structure establishes what could be considered one of the most vital qualities of an ESN, substantial and regular leadership involvement.

Rule Five (provide positive role models wherever possible) lists *select personnel to serve as role models* and *explain the responsibilities of a role model* to represent the Remembering and Understanding Columns under the Emerging Group. The Developing Group consists of the Applying and Analyzing columns and they state *demonstrate the responsibilities of a role model* and *examine the duties of a role model.* The most advanced ESNs will operate under the Mastering Group and *prioritize the need for role models in the ESN process* and *Develop a sustainability plan for role models* represent the Evaluating and Creating columns.

Rule Six (consistently reward knowledge sharing behavior) is a fundamental function of any activity. Positive reinforcement is a powerful motivator and can significantly contribute to sustained success. The Emerging Group with the Remembering and Understanding columns states *define knowledge sharing behavior* and *Illustrate examples of knowledge sharing behavior*, respectively. The Applying and Analyzing columns state *model the best examples of knowledge sharing behavior* and *examine best practices of knowledge sharing behavior* that comprise the Developing Group. The Mastering Group consists of the Evaluating and Creating columns and they state *prioritize the need for knowledge sharing behavior* and *generate a culture of support for knowledge sharing.*

Lastly, strategic scoring is a vital element of this rubric, as it is the informative deliverable and has the potential to address the challenges outlined earlier in this thesis. The configuration of the scoring emphasizes improving maturity and provides a pathway

to achieve that goal. It is important to note that each step associated with each rule is tied to an action. This interconnection requires participating ESNs to tie their activities associated with the rubric to perform a specific performance task related to each phase but grants them the latitude to move at their own pace and address each rule independently.

The next chapter puts the rubric into practice to assess three ESNs as case studies, all of which are versions of a wiki.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. CASE STUDIES

## A. INTRODUCTION

The HSE, as a discipline, does not currently have an ESN. An ESN in the form of a wiki is a proven way to create a BoK, which is needed for the discipline to mature. Collective intelligence, namely an ESN, and in this case, crowdsourced via a wiki, is a proven collaborative platform and is a viable option as a HS wiki or similar ESN to develop a BoK.

This chapter applies the rubric to three existing wikis, Wikipedia, the U.S. Patent and Trademark Office's (USPTO) Peer-to-Patent and the DNI's Intellipedia. The mechanics of the rubric are fairly simple despite the complexity involved in its development. Evidence of the highest maturity is applied to each question and a point value is assigned to that level of maturity. The higher the score, the greater the maturity of the ESN.

## B. WIKIPEDIA

### 1. Background

While wikis have been around for decades and serve as a way to sustain a group conversation, Wikipedia advanced the capability into a collating function with the intent of building a reference resource, "with a large, disparate online community spanning language and geography."[151]

Wikipedia is easily the most famous of all wikis. It was the creation of Jimmy Wales and Larry Sanger and was launched on January 15, 2001. The name came from a combination of the words "wiki," a Hawaiian word for "quick," and "encyclopedia."[152] Wikipedia could be considered the purest form of a wiki as described by Reagle in *Good Faith Collaboration—The Culture of Wikipedia* as a "potent collaboration tool that

---

[151] Phoebe Ayers, Charles Matthews, and Ben Yates, *How Wikipedia Works: And How You Can Be a Part of It* (San Francisco: No Starch Press, 2008), Kindle locations 1170–1172, Kindle edition.

[152] *Wikipedia*, s.v. "Wikipedia," last modified December 7, 2016, https://en.wikipedia.org/wiki/Wikipedia.

permits asynchronous, incremental a transparent contributions from many individuals."[153]

Wikipedia has more than five million articles in the English language version and over 40 million articles in 293 languages covering all manner of topics from basic science to accounts of television show episodes.[154]

Wikipedia defines an article as "a Wikipedia page that contains encyclopedic information."[155] This simplicity keeps participants contributing and the whole process moving.

The page structure of Wikipedia encourages short articles instead of longer ones because the pages are hypertext, and as such, are linked to other related articles. This structure eliminates the need for extensive footnoting and indexes a print encyclopedia requires.[156]

The best articles attribute any statement of fact to a source outside of Wikipedia no matter who originally created the article, which differentiates Wikipedia from other encyclopedias. Each fact is linked to an outside source to illustrate from where the information originates.[157]

This approach allows for the best possible articles. Ones with a long list of sources meet the most interesting utility of Wikipedia. They serve as excellent starting points for research. Another function of the verifiability policy is to assist the editors in reviewing articles. If a fact is not cited, the editor can easily determine if it is from outside sources and mark it accordingly.[158]

---

[153] Joseph M. Reagle and Lawrence Lessig, *Good Faith Collaboration: The Culture of Wikipedia*, (Cambridge, MA: MIT Press, 2012), Kindle locations 140–141, Kindle edition.

[154] *Wikipedia*, s.v. "Wikipedia: Size Comparisons," last modified November 16, 2016, https://en.wikipedia.org/wiki/Wikipedia:Size_comparisons.

[155] Ayers, Matthews, and Yates, *How Wikipedia Works: And How You Can Be a Part of It*, Kindle location, 280.

[156] Ibid., 968–972.

[157] Ibid., 452–456.

[158] Ibid., 459–463.

Wikipedia's policy of no original research means all articles should not "contain original ideas, conclusions, descriptions or interpretations of facts" nor should they "contain editors' personal views, political opinions or any unpublished analysis of published material."[159]

The neutral point of view policy is the central, oldest, and most respected in Wikipedia, and insists all points of view on a topic should be represented fairly. This viewpoint concentrates the purpose of the article on information as opposed to influencing.[160]

Is Wikipedia accurate? Last year, *Nature* published a survey comparing forty-two entries on scientific topics on Wikipedia with their counterparts in Encyclopedia Britannica. According to the survey, Wikipedia had four errors for every three of Britannica's, a result that, oddly, was hailed as a triumph for the upstart. Such exercises in nitpicking are relatively meaningless, as no reference work is infallible."[161]

Britannica refuted the finding and issued a statement that said, "Britannica has never claimed to be error-free. We have a reputation not for unattainable perfection but for strong scholarship, sound judgment, and disciplined editorial review."[162] Britannica's president Jorge Cauz has cautioned Wikipedia to use editorial oversight, as it would "decline into a hulking mediocre mass of uneven, unreliable, and, many times, unreadable articles."[163] Wales has said that he would consider Britannica a competitor, "except that I think they will be crushed out of existence within five years."[164]

The American Library Association (ALA) published an article in 2010 in which it praised Wikipedia, "I am reminded that Wikipedia is one of the most visited websites on the Internet today. For this reason alone, we librarians must respect the fact that some

---

[159] Ayers, Matthews, and Yates, *How Wikipedia Works: And How You Can Be a Part of It*, Kindle locations, 476–479.

[160] Ibid., 505–508.

[161] Ibid., 510–513.

[162] Stacy Schiff, "Know It All," *The New Yorker*, July 31, 2006, http://www.newyorker.com/magazine/2006/07/31/know-it-all.

[163] Ibid.

[164] Ibid.

things people find on Wikipedia are useful. For one, if someone is looking for basic information on the French Revolution—a simple one or two sentence fact—and they do not have a lot of time to spend researching, where do they go? Wikipedia."[165]

### 2. Applying the Rules and Supporting Evidence

This section illustrates the process for applying evidence to answer the six questions and then those results are used to establish an overall score for the ESN.

Rule One. Allow cultural change over time.

*Score: 6—Design cultural adaptation into the ESN.*

Wikimedia, Wikipedia's organizing body, meets the criteria of a large social movement with the goal of making knowledge freely available to everyone with an internet connection while also being an intellectual movement by advocating free information access and open licensing. It aligns different interests of the academic, educational, social, and political worlds. While doing so, it also bears the hallmarks of a traditional open source project be being "slightly anarchist, without a clear hierarchy, and highly dependent on participative organizational designs."[166]

More simply put, "Wikipedia is building a huge compilation of materials and facts, many of which come from traditional sources, with the content policies simply acting as standards applied to everything submitted. Thinking of Wikipedians as the new encyclopedists makes sense, but, saying it more precisely, they're engaged in creating a new kind of tertiary source, for a networked world, delivered free."[167]

Wikipedia has what is referred to as the "Five Pillars of Wikipedia" that are the fundamental rules that guide the site. They are "Wikipedia is an encyclopedia (not anything else), Wikipedia has a neutral point of view (the NPOV policy), Wikipedia is

---

[165] Travis Bonnett, "In Defense of Wikipedia: An Editorial," American Library Association, May 2010, http://www.ala.org/nmrt/news/footnotes/may2010/in_defense_of_wikipedia_bonnett.

[166] Dariusz Jemielniak, *Common Knowledge?: An Ethnography of Wikipedia* (Stanford, CA: Stanford University Press, 2014), 117, Kindle edition.

[167] Ayers, Matthews, and Yates, *How Wikipedia Works: And How You Can Be a Part of It*, Kindle locations, 1446–1449.

free content that anyone may edit. (All Wikipedia content is freely licensed and free of charge, and content is freely editable,) Wikipedia has a code of conduct. (Editors should behave civilly toward each other,) Wikipedia does not have firm rules. (The editing community can change the rules.)"[168]

Rule Two. Create opportunities for people to get to know one another.

*Score: 5—Defend innovative networking.*

What distinguishes Wikipedia from other encyclopedic projects is its sheer scope with no limitations or defined area of knowledge. It merges the work of both specialists and generalists linked into an integrated effort. Another advantage of Wikipedia is the dynamic nature of the articles. The content of any article could change from minute to minute, which is made possible by eliminating the outdated requirement to have an expert-generated article.[169]

Rule Three. Focus on connecting people over gathering content.

*Score: 4—Attribute value to connecting people.*

Wikipedia operates under the principle of "if you can see it, you can edit it."[170] Information is provided in the form of articles posted by contributors on any topic to be viewed by anyone with an internet connection and a web browser. Readers can create an account that allows them to log in and bookmark pages of interest, discuss edits to a page, or view the history of an article to see how the article has evolved over time. Wikipedia allows readers to organize articles into categories that, in effect, create indexes of a larger general topic. In turn, editors review articles and ensure they are following the rules established by administrators. Almost everyone in this process is an unpaid volunteer.

---

[168] Ayers, Matthews, and Yates, *How Wikipedia Works: And How You Can Be a Part of It*, Kindle locations, 8024–8028.

[169] Ibid., 980–984.

[170] Reagle and Lessing, *Good Faith Collaboration: The Culture of Wikipedia*, Kindle location 101.

The three most vital policies to Wikipedia are verifiability, no original research, and NPOV.[171] Verifiability means that any contribution should be cited from an external source. Those not cited are flagged as such so that readers can tell. No original research means academics cannot simply publish to Wikipedia and assert their research as fact. Other wiki-type sites can be used for this type of assertion. NPOV is simply that. No article should take a one-sided view of a topic. These vital policies create the environment for good content to be created with minimal editorial control.[172]

Rule Four. Top-down support of bottom-up solutions.

*Score: 6—Integrate leadership into bottom-up problem solving.*

Jimmy "Jimbo" Wales is the co-founder of Wikipedia and this quote is a good example of his leadership philosophy where he has limited some capability of editing, "Not every case of allowing more people to edit would count as "more open." For example, if we had a rule that 'Only Jimbo is allowed to edit this article' then this would be a lot LESS open than "no one is allowed to edit this article." Openness refers not only to the number of people who can edit, but a holistic assessment of the entire process. I like processes that cut out mindless troll vandalism while allowing people of diverse opinions to still edit. Those are much better than full locking."[173]

This quote is a good example of Wales' approach to leadership. He keeps his opinions to himself until absolutely necessary and then he is obliged to provide extensive justification when he does.

It is one thing to resist exerting force in a collaborative environment; it is another to support guidance from participants vigorously, which is exemplified in the following quote from Wales, "I know it is bad form to quote an entire post just to say 'me too' but I wanted to say that Daniel is right on the money here, and displays plays what I think of as

---

[171] Ayers, Matthews, and Yates, *How Wikipedia Works: And How You Can Be a Part of It*, Kindle locations, 5586–5587.

[172] Ibid., Kindle locations 425–427.

[173] Reagle and Lessig, *Good Faith Collaboration: The Culture of Wikipedia*, Kindle locations 1157–1160.

true Wikipedia spirit. We have to have a passion to 'get it right' or we'll be full of rampant nonsense."[174]

Rule Five. Provide positive role models wherever possible.

*Score: 6—Develop a sustainability plan for role models.*

A police force of sorts exists within Wikipedia. These experienced editors clean up vandalism, review edits from anonymous or new editors, and otherwise keep order with noteworthy speed and regularity. Many would-be vandals are surprised to find their work is removed within minutes. This role is important and contributes to the solidity of Wikipedia since, "dense networks provide social rewards for those punishing norm violators, and promoting Wikipedia as agile in correcting its mistakes."[175]

The millions of users are the key to Wikipedia's resiliency. When an article is vandalized, anyone who has "followed" that article will be notified of a change. They could go back to the article and engage the vandal in a conversation in the talk page. If no discussion occurs, the editor can change it back. If the vandalism continues, the article could be locked with edits having to be reviewed before changes are made. "Gardeners" are those who are not necessarily authors of articles but enjoy going through articles and tidying them up to correct spelling, grammar and punctuation, for example. They may remove vandalism as well.

While Wikipedia is open to everyone, some roles have emerged to illustrate individual contributions and experience. In descending order, they are steward, checkuser, oversighter, bureaucrat, administrator, rollbacker, registered user, new user, unregistered user, and blocked user.[176]

The blocked user, unregistered user, and new user have restricted rights as compared to a registered user to promote registration and limit time consuming disruptive

---

[174] Reagle and Lessig, *Good Faith Collaboration: The Culture of Wikipedia*, Kindle locations, 1649–1651

[175] Jemielniak, *Common Knowledge?: An Ethnography of Wikipedia*, 14.

[176] Ibid., 24.

behavior. The rollbacker has access to tools that clean up vandalism and other problematic contributions.[177]

Administrators are the day-to day management of Wikipedia and grant and revoke privileges to users.[178] They are the largest of the groups and are experienced users with important prerogatives. They have the authority to block and unblock users, delete and restore content, and protect articles from editing.[179]

Bureaucrats have administrative authority to grant additional privileges to registered users and have technical responsibilities guided by community consensus. Oversighters have the authority to hide revisions and other entries related to an article so that only oversighters and stewards can see them.[180]

Checkusers do just that. They are permitted to investigate IP addresses of users to confirm one user is not editing articles from multiple accounts.[181] Stewards have unlimited access to all projects and can perform any task. Only a very select few have this much power.[182]

Rule Six. Consistently reward knowledge sharing behavior.

*Score: 2—Illustrate examples of knowledge sharing behavior.*

The use of barnstars as a form of recognition among editors is very important to the overall community. Barnstars are virtual awards handed out from peer to peer as recognition of unusually good work. This authentic kind of recognition also drives productivity and is an integral part of Wikipedia's success.[183]

---

[177] Jemielniak, *Common Knowledge?: An Ethnography of Wikipedia*, 26.

[178] Ibid.

[179] Ibid., 26–27.

[180] Ibid., 25.

[181] Ibid.

[182] Ibid.

[183] Ibid., 18.

### 3. Conclusion

Wikipedia's cumulative score across all of the rules is 29. It scored highest in rules one—allow cultural change over time, four—top-down support of bottom-up solutions, and five—provide positive role models whenever possible. All these rules scored a maximum of six. The lowest score was a two in rule six—consistently reward knowledge-sharing behavior.

## C. PEER-TO-PATENT

### 1. Background

The USPTO describes itself as, "the federal agency for granting U.S. patents and registering trademarks. In doing this, it fulfills the mandate of Article I, Section 8, Clause 8, of the Constitution that the legislative branch 'promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.' The USPTO registers trademarks based on the commerce clause of the Constitution (Article I, Section 8, Clause 3)."[184] Essentially, the U.S. government agency defends intellectual property and promotes innovation by granting 20-year monopolies to creators of novel inventions.

Novel is the operative word. An examiner needs to research "prior art" or what has existed before the invention to determine if the invention has advanced a product enough to be considered unique, which takes between 15 and 20 hours to complete.[185] Roughly 2 million patents are in existence with millions more applications for patents.[186] The problem is simple; not enough examiners are available, the research is very technical, and no standard database exists to support the research.

---

[184] "About Us," February 12, 2015, http://www.uspto.gov/about-us.

[185] Beth Simone Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful* (Washington, DC: Brookings Institution Press, 2009), 5, Kindle edition.

[186] Ibid.

The purpose of Peer-to-Patent is to significantly improve the patent approval rate and reduce the patent application backlog by outsourcing the prior art research from overwhelmed and inexperienced examiners to a self-appointed team of experts.

The following example derives from Beth Noveck's *Wiki Government* that answers how information is shared, with whom, and why.

Steve Pearson is an employee of a large technology company participating in the Peer-to-Patent pilot. The company has a vested interest in participating for a few reasons. First, it can defend its existing patents by providing it prior art. Second, it can see what is being submitted for patents and can plan for upcoming innovations even if it does not belong to the company. Finally, it speeds up the entire patent review process, which is good for everyone seeking a patent, to include Steve's company.[187]

Steve agrees to participate in Peer-to-Patent, goes to the website (www.peer totpatent.org), creates an account by providing some basic information like his name and email address along with establishing a user name and password. He also has the option to add profile information about himself, his background and education, as well as his expertise. This information speeds up the "getting to know you" process when it comes time to work with his review group on his selected application. Steve then picks his area of interest, and in his case, it is database technology.[188]

While a pilot, companies elect to participate and are then vetted by the USPTO. The New York Law School provides staffing for this process and manages the list of available patent applications.[189] Hewlett-Packard has submitted an application that interests Steve. He selects it and begins his review process by reading the application and engaging the other members who have volunteered to review it as well.[190]

Steve can see his team of reviewers and has a sense of their backgrounds. The team has 29 people consisting of four engineers, 13 technologists, five lawyers, two

[187] Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, 73.

[188] Ibid.

[189] Ibid.

[190] Ibid.

students, two academics, a New York Law School research assistant keeping an eye on the group interaction, and two others.[191]

The group ultimately submitted nine pieces of prior art to include old patents, a computer program, and a computer manual from the Intel Corporation. The Peer-to-Patent software requires the prior art be cited by the pages, paragraphs, and phrases relevant to the claims of the patent application, as well as explaining its relevance.[192]

All this information assists the patent examiner but the most significant contribution of Peer-to-Patent is the exacting citation requirement. While illegal in the paper-based system, it is legal via Peer-to-Patent and is very useful to the USPTO.[193]

### 2. Applying the Rules and Supporting Evidence

Rule One. Allow cultural change over time.

*Score: 3—Build a process to support culture change.*

The objective of Peer-to-Patent was simple in execution but daunting in impact. It was essentially an internet-based jury. Technically, it was very straightforward. The daunting task was to convince an entrenched bureaucracy to change fundamental practices that have been in place for decades. This kind of change is only possible through building consensus and emphasizing filling information deficits and lessening the workload.[194]

Rule Two. Create opportunities for people to get to know one another.

*Score: 3—Develop a plan for networking.*

Experts are invited by Peer-to-Patent staff or are referred by other experts. They are granted access to the site through a user name and password once they are accepted as application reviewers. It is a very small participant population especially during this pilot.

---

[191] Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, 76.

[192] Ibid., 77.

[193] Ibid., 77–78.

[194] Ibid., 91.

The number of examiners totaled only a little over 100 with 125 applications with a little over 2,300 peer reviewers.[195] Compared to Wikipedia's millions of participants and articles, Peer-to-Patent's access concerns are miniscule.

Rule Three. Focus on connecting people over gathering content.

*Score: 4—Attribute value to connecting people.*

Information is processed more than it is shared in Peer-to-Patent. The applicants upload their application to the Peer-to-Patent website and then wait for the application to be reviewed. Next, groups of volunteer experts go to website and select an application they want to assist with and begin the research process looking for prior art. The results of the research, either proof of prior art or not, are submitted to the website and reviewed by the examiner and a final adjudication is provided to the applicant.[196]

Daren Brabham in his work on crowdsourcing refers to Peer-to-Patent as, "evidence that the government can effectively mobilize citizens to solve specific problems through a crowdsourcing arrangement."[197]

Rule Four. Top-down support of bottom-up solutions.

*Score: 2—Illustrate the benefit of top-down support to bottom-up solutions.*

Leadership at the USPTO focused on technology that was very supportive of Peer-to-Patent and the idea of an ESN. This leadership was willing to suspend its typically top-down hierarchical approach and allow the Peer-to-Patent team to accept "rough consensus and running code;" that is, asking one of the most conservative, independent, process-oriented institutions to experiment with its core operations.[198]

Gaining and maintaining the trust of senior leadership and SMEs is vital to the survival of such a project.

---

[195] Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, 73.

[196] Ibid., 79.

[197] Brabham, *Crowdsourcing*, Kindle locations 566–576.

[198] Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, 93.

Rule Five. Provide positive role models wherever possible.

*Score: 1—Select personnel to serve as role models.*

Peer-to-Patent has divided work into tasks and then allows the members to divide the tasks among themselves. The members need to self-select roles to accomplish the work effectively.[199] The challenging questions asked by the project is the best way to keep them engaged in the ESN. "With patent review, it is particularly easy to "chunk" the work into manageable, discrete tasks that makes collaboration possible, because the questions are already well identified as a matter of law."[200]

Rule Six. Consistently reward knowledge sharing behavior.

*Score: 6—Generate a culture of support for knowledge sharing behavior.*

There are intrinsic motivations for both individuals and organizations. Individually, Peer-to-Patent motivates the examiners by improving an antiquated system and reducing their rate of review. The peer reviewers are motivated intrinsically by sharing their expertise, improving a process they may be interested in and growing their professional network.[201] The applicants are motivated to participate by the "head of the line" privilege participation brings which ultimately shortens the wait time for patent approval.

### 3. Conclusion

Peer-to-Patent is a great example of an impactful use of wiki to achieve a very specific goal by tapping into a community of volunteer SMEs. It is unfortunate the Peer-to-Patent project was not sustained beyond the test period. It can be inferred that the political support was insufficient.

---

[199] Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, 83–84.

[200] Ibid.

[201] Ibid., 176.

## D. INTELLIPEDIA

### 1. Background

In 2004, D. Calvin Andrus wrote a paper titled, *The Wiki and the Blog—Toward a Complex Adaptive Intelligence Community.* Andrus asserts, "We must transform the Intelligence Community into a community that dynamically reinvents itself by continuously learning and adapting as the national security environment changes."[202] He goes on to extol the virtues of a wiki and describes them as "self-organizing knowledge websites."[203] This concept is the inspiration for Intellipedia.

Andrus underpins his assertion using complexity theory and its associated theories, general system theory, information theory, chaos theory, and fractal theory, to establish the academic rigor that supports his approach.[204] This description is followed by an explanation of the six critical components of complex adaptive systems: self-organization, emergence, relationships, feedback, adaptability, and non-linearity.[205]

Andrus cites Wikipedia as an example, "In sum, from the little bits of work by many, many people, following simple rules of content contribution and editing, the most comprehensive and authoritative, and bias-free encyclopedia in the world has been produced in four years. This is an encyclopedia that is dynamically and constantly changing in response to the world as the world itself is changing."[206]

Andrus then proposes, in conjunction with a blog, the development of an IC wiki. The purpose of the intelligence wiki would be to refine the vast repository of data and databases to make it more adaptable. He also recommends search and feedback functions to increase the impact of this construct.[207]

---

[202] Andrus, D. Calvin. "The Wiki and the Blog," *Intelligence* 49, no. 3 (2005): 2.

[203] Ibid., 15.

[204] Ibid., 3–4.

[205] Ibid., 8–9.

[206] Ibid., 16.

[207] Ibid., 18.

The process of feedback is vital to such a system. While the general concept of sharing information is important, it is also important to understand who is providing and who is consuming what information.[208] Intellipedia is available on all networks of all classifications around the world allowing a critical mass to form and drive collaboration.[209]

Vital components of successful virtual communities are critical mass, trust, content, and purpose.[210] Critical mass, as previously discussed, centers on giving every available person access to the community to include the policy officers. The community flourishes only with regular participation by a wide variety of disciplines. Granting as many participants as easy access as possible is vital to the best possible collaborative experience.[211]

Trust is reliant on tradecraft. The technical tradecraft secures the network, tools, and data. Procedural tradecraft makes the rules of use explicit and accessible. Security tradecraft establishes who has access to the systems. Since the systems were preexisting, granting access was uncomplicated. Ultimately, all the tradecraft rules must be uncomplicated.[212] Content is the lifeblood of the system and initially content will need to be generated en masse by a dedicated cadre to create the necessary breadth and depth to keep participants engaged.[213] Senior leaders and their level of participation in the process ultimately drive purpose. Articles by and commented on by them will drive interest.[214]

> Intellipedia (https://www.intelink.gov/wiki) is an online system for collaborative data sharing used by the United States Intelligence Community (IC). It consists of three different wikis with different levels of classification: Top Secret, Secret, and Sensitive but Unclassified. They are used by individuals with appropriate clearances from the 16 agencies of the IC and other national-security-related organizations, including

[208] Calvin, "The Wiki and the Blog," 19.

[209] Ibid., 21.

[210] Ibid.

[211] Ibid., 21–22.

[212] Ibid., 22.

[213] Ibid.

[214] Ibid.

> Combatant Commands and other federal departments. The wikis are not open to the public.[215]

Andrus addresses the purpose of Intellipedia by listing what he sees as the needs of the intelligence community.

> We need a space for change that is not organization dependent (remember, reorganizations are not part of the solution set). We need a space to begin implementing the five mission changes that is independent of organization. We need a space that is open not just to the IC but also to other non-intelligence national security elements—to allow sharing and feedback. We need a space with a sufficiently large critical mass of intelligence officers. We need a space that is neither organizationally nor geographically nor temporally bound. We need a secure space that can host a corporate knowledge repository. We need a flexible space that supports tools for self-organizing (Wiki), information-sharing (Blog), searching, and feedback as previously mentioned. We need a place in which tradecraft procedures can be implemented. In short, we need a space that is always on, ubiquitously distributed, and secure. We need an electronic network. We need SIPRNet.[216]

This list clearly established the groundwork for the development and purpose of Intellipedia.

The information being shared is specifically by and for the USIC. As such, the information is specifically germane to their interests and needs. The annual threat assessment produced by the DNI and discussed in the literature review outlines all the areas of interest to the USIC.

Intellipedia uses the same MediaWiki software used by Wikipedia and the pages look very similar to Wikipedia as well. The same structure also exists for contributing and editing of articles as well. The only difference in this regard is very specific attribution given to the submitter and editor.[217]

Criticism of Intellipedia specifically is virtually nonexistent. The complaints associated with Intellipedia are similar to any wiki. They include but are not limited to

---

[215] Jessica Keyes, *Enterprise 2.0: Social Networking Tools to Transform Your Organization* (Boca Raton, FL: CRC Press, 2012), 25.

[216] Calvin, "The Wiki and the Blog," 20.

[217] Keyes, *Enterprise 2.0: Social Networking Tools to Transform Your Organization*, 25.

resistance to change of any kind, attempting to cling to a "need to know" vice a "need to share" mentality, unfounded concerns about access control while Intellipedia resides on existing and well-established networks and concern about analyst productivity when contributions to Intellipedia are not considered production.

Intellipedia is the closest conceptually to what could work as an ESN for the HSE. The most notable characteristic is the practice of attribution. It creates a more specific link to the users contributing to an article. Its inherent value simply allows someone seeking information on a topic to have direct access to those providing it. Some could argue it is a fundamental function of the concept of HS, creating a network of expertise to support the entire enterprise efficiently and accurately.

### 2. Applying the Rules and Supporting Evidence

Rule One. Allow cultural change over time.

*Score: 3—Build a process to support culture change.*

The DIA report illustrated a best practice that could aid in the initial population of content with a HS Wiki. "Some contributors develop completely new content, while others 'borrow' from Wikipedia as a starting point, then elaborate in the Intellipedia environment to create articles that are relevant for intelligence analysts."[218] Crossing high quality HS-related articles over from Wikipedia would expedite the process of accumulating useful data into a HS Wiki. The caveat to this action is those crossing data over would be required or at least encouraged to confirm the quality of the articles, as those articles would be attributed to them.

Rule Two. Create opportunities for people to get to know one another.

*Score: 3—Develop a plan for networking.*

The policy discussion intent of Intellipedia negates the need for a Wikipedia-like NPV policy. This approach allows for a new method of information sharing. Many

[218] Nancy M. Dixon and Laura A. McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency* (Arlington, VA: DIA Knowledge Laboratory, 2008), 11–12.

offices across the community use the wiki to simply maintain and transfer knowledge regarding daily operations.[219]

A unique function within Intellipedia that differs greatly from Wikipedia is all activity is attributed to a specific person. Contributions cannot be anonymous. An amusing quote from the former Deputy Director for National Intelligence for Analysis, Thomas Fingar commenting on Intellipedia during a talk to the Council on Foreign Relations states, "It's the Wikipedia on a classified network, with one very important difference: it's not anonymous. We want people to establish a reputation. If you're really good, we want people to know you're good. If you're making contributions, we want that known. If you're an idiot, we want that known too."[220] This statement clearly illustrates the intent and desire to improve the quality of the USIC analyst corps through this kind of attribution.

The DIA report on Intellipedia concludes with a keen observation about the potential of Intellipedia to address some longstanding issues within the USIC. "The interviewees' responses raise interesting questions about the disruptive potential of so-called 'social software' on organizational norms and practices in the intelligence community. However, our work indicates that social software like Intellipedia could dramatically enhance the development of cooperative and collaborative networks among intelligence analysts across organizational boundaries."[221]

The DIA report answered this question in significant detail. They felt it went beyond an online encyclopedia and reflected all the crowdsourcing types to varying degrees. They found it certainly addressed knowledge discovery and management but were surprised it quickly went beyond that simple task. They found users immediately used the search function frequently and advertised the need for information in articles

---

[219] Keyes, *Enterprise 2.0: Social Networking Tools to Transform Your Organization*, 26.

[220] Thomas Fingar, "Intelligence Reform [Rush Transcript; Federal News Service]," Council on Foreign Relations. March 18, 2008, http://www.cfr.org/intelligence/intelligence-reform-rush-transcript-federal-news-service/p15754.

[221] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 4.

they provided. This approach essentially not only provided answers but drove continued participation by asking questions as well.[222]

Rule Thre. Focus on connecting people over gathering content.

*Score: 3—Demonstrate the difference between connecting people vice capturing content.*

The most recent publically available usage statistics show the top-secret version of Intellipedia has the most activity with 255,402 registered users, 113,379 pages, 290 million views, and 6.2 million edits. The secret version is next with 214,801 registered users, 107,349 pages, 246 million views, and 3.4 million edits. The unclassified version of Intellipedia is the least utilized of the three with 127,294 registered users, 48,274 pages, 94 million views, and 1.4 million edits.[223]

The DIA report on Intellipedia illustrates this level of activity very well.

> At the same time that Intellipedians are developing and projecting their own presence into the virtual world of intelligence, they are using Intellipedia and blogs to gather contextual information on their peers. For example, one of the ways analysts determine the validity of an Intellipedia page or change is to click on the author's link and look at their background. This frequently brings the reader to the contributor's blog: as several of our interviewees pointed out, it is not unusual for people who contribute to Intellipedia to maintain a blog, and to provide Intellipedia links to their Intelink blogs. The blogs provide a place for people to establish their identity. As one heavy Intellipedia user told us, people check his blog to see if he has the right credentials for the work he is doing: Does this person have the experience about this specific issue to be credible?[224]

Rule Four. Top-down support of bottom-up solutions.

*Score: 2—Illustrate the benefit of top-down support to bottom-up solutions.*

---

[222] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 11.

[223] Jason Smathers, "Intellipedia Usage Statistics," MuckRock, January 28, 2014, https://www.muckrock.com/foi/united-states-of-america-10/intellipedia-usage-statistics-10058/#file-16141.

[224] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 9–10.

The DIA report illustrated the information-sharing components of Intellipedia. They found it interesting that community of practice pages were popular as collaboration spaces connecting several agencies. Another observation involved managerial approaches to contribution support. Some managers were hands on and specific in what to share while others were supportive of contribution but vague in what should be shared.[225]

Rule Five. Provide positive role models wherever possible.

*Score: 5—Explain the responsibilities of a role model.*

The DIA report supports this approach. "In fact, the users we spoke with were typically very excited about the way Intellipedia affords them the opportunity to publicize their work and interests across the larger IC."[226]

One of the more powerful characteristics of Intellipedia in comparison to Wikipedia is the practice of attribution. That all users' contributions can be linked back to them by name and email address cannot be overstated. This loss of anonymity is a powerful benefit considering the purpose of Intellipedia is not to simply accumulate data for reference but to drive policy discussions across the USIC. Thus, a form of peer vetted creative production is created where a more pronounced feedback loop is used, which is absent in Wikipedia.[227]

Rule Six. Consistently reward knowledge sharing behavior.

*Score: 6—Generate a culture of support for knowledge sharing behavior.*

Andrus received the Galileo Award from the Central Intelligence Agency (CIA) for his paper, *Wiki and the Blog: Towards a Complex Adaptive Intelligence Community*, which describes what would eventually become Intellipedia.

In 2009, Don Burke and Sean Dennehy received the Homeland Security Service to America Medal from the Partnership for Public Service for, "for their unrelenting

[225] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 8.

[226] Ibid., 6.

[227] Ibid., 11.

dedication to promoting and expanding information-sharing in the Intelligence Community."[228]

Similar to Wikipedia's barn stars, Intellipedia "gardeners" receive virtual and actual shovels as recognition for their thankless work maintaining order within the site.[229]

A practice common to both Wikipedia and Intellipedia is the practice of placing featured articles on a front page. Noteworthy articles are selected by a board of peers and are run on the front page for a period of time. This practice serves a few functions. First, it serves as an example to other users what the best article should look like. Second, it brings notoriety to the contributors and their organizations, and in some cases, it may be tied to performance plans and awards.[230]

### 3. Conclusion

Applying the rules and the rubric to these case studies has resulted in a better understanding of the strengths and the weaknesses of each platform, but more importantly, each operator of the platforms now has a path forward to improvement. Table 2 shows the results of the assessment.

---

[228] "Intellipedia Gurus Win 2009 Homeland Security Medal," Central Intelligence Agency. April 30, 2013, https://www.cia.gov/news-information/featured-story-archive/intellipedia-homeland-security-medal.html.

[229] Eugene Eric Kim, "Intellipedia Shovel," Eugene Eric Kim Comments, September 27, 2006, http://eekim.com/blog/2006/09/intellipedia-shovel/.

[230] Dixon and McNamara, *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 14.

Table 2. ESN Rubic Results.

| The Rules | 1. Allow cultural change over time. | 2. Create opportunities for people to get to know one another. | 3. Focus on connecting people vice capturing content. | 4. Top-down support of bottom-up solutions. | 5. Provide positive role models wherever possible. | 6. Consistently reward knowledge sharing behavior. | Totals |
|---|---|---|---|---|---|---|---|
| **Wikipedia** | 6 | 5 | 4 | 6 | 6 | 2 | 29 |
| **Peer-to-Patent** | 3 | 3 | 4 | 2 | 1 | 6 | 19 |
| **Intellipedia** | 3 | 3 | 3 | 2 | 5 | 6 | 22 |

As Table 2 shows, Wikipedia is the most mature of the three cases with a score of 29, Peer-to-Patent is the least mature with a score of 19, and Intellipedia is in the middle with a score of 22. Wikipedia's highest scores were in allowing cultural change (Rule One), top-down support of bottom-up solutions (Rule Four), and providing role models wherever possible. In all these rules, Wikipedia had the highest score possible with a score of six. Wikipedia scored lowest in consistently rewarding knowledge sharing behavior (Rule Six).

Peer-to-Patent scored the highest in consistently rewarding knowledge-sharing behavior (Rule Six) and scored the lowest in providing positive role models wherever possible (Rule Five). Intellipedia also scored the highest at rewarding knowledge-sharing behavior (Rule Six) but scored the lowest in the top-down support of bottom-up solutions (Rule Four).

While these scores are informative, the rubric serves an additional purpose. It serves to provide directions for improvement. For example, the lowest score of all the cases is Peer-to-Patent's rule five of one. Peer-to-Patent can seek to improve along that line by using the rubric. It can explain the responsibilities of a role model to rise to a score of two or it can plan and resource to develop a sustainability plan for role models to achieve a score of six.

It cannot be overstated how important it is for the highest echelons of leadership to endorse not only a HS Wiki or similar ESN, but to vigorously support and participate in the day-to-day functions to the point that they are as ubiquitous as Wikipedia within the HSE. The disruptive nature of these kinds of changes can be difficult in the best of circumstances, and when these changes are not messaged and resourced adequately, it is even more difficult.

The next chapter combines the function of the rules and the rubric with the results of the case studies to show the effectiveness of the ESN rubric to guide the development of a HS-centric ESN.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. FINDINGS

The purpose of this research is to validate a system to improve the connectedness of the HSE by providing rules and a rubric to guide an ESN to a condition of maturity. In the interest of managing the scope and complexity of the research, the ESN was given the objective of creating a HS BoK using a wiki. The value of the BoK to the HSE would be the establishment of a formal and adaptive repository of reference material that could be constantly updated and expanded as necessary.

The ESN rules were developed to serve as a base for the ESN rubric. The rules are based on existing and established research in the knowledge management discipline. The rubric was developed by adapting Bloom's Taxonomy to the rules and was designed to serve two purposes. The first is to assess existing ESNs to establish their maturity and guide their development. The second, and more important, is to serve as a template to assist in the planning of new ESNs.

Each of the case studies was selected for different reasons. Wikipedia was chosen for not only its ubiquity but also for its proven and established culture. The USPTO Peer-to-Patent was chosen for the audacious nature of the project. Despite being a pilot, and not currently a functioning wiki, Peer-to-Patent explored using an ESN to solve a daunting information-sharing problem faced by the U.S. government. Intellipedia was selected because it was the closest example of the application of a wiki-based HSE ESN.

Applying the rubric to Wikipedia results in a cumulative score of 29 out of a possible 36. This score was the highest of all the cases. As observed in the case studies, Wikipedia scored the highest with questions one, four, and five. As such, Wikipedia is designed for cultural adaptation, integration of leadership into problem solving and the development of a sustainability plan for role models. Question two received the next lowest score. Wikipedia defends innovative networking but does not have methods to improve networking. Question three attributed a value to connecting people. Question six had the lowest scoring question in which Wikipedia only illustrates examples of knowledge sharing.

For questions two, three, and six, Wikipedia could use the rubric to plan improvements, such as developing methods to improve networking, develop an assessment methodology to determine the quality of interpersonal connections, or create models of best practices of knowledge-sharing behaviors to advance from one column to the next.

The rubric application to Peer-to-Patent was somewhat different. Peer-to-Patent's cumulative score was 19 out of 36, which is the lowest case score and a good example of how to use the rubric to plot a prioritized path forward for a struggling ESN. The rules are roughly prioritized from the most impactful to least impactful although it is not possible to establish priority objectively. Nonetheless, the rubric can serve as a guide to improvement. USPTO could follow a number of approaches to improve Peer-to-Patent. The two ends of the spectrum are gradual or dramatic changes.

The gradual approach for improvement of Peer-to-Patent is to (rule one) examine the pace of cultural adaptation, (rule two) categorize the degree of connectedness, (rule three) assess the quality of interpersonal connections, (rule four) develop a process to streamline solution support, and (rule five) explain the responsibilities of a role model. Rule six is already at the top of the scale.

The dramatic approach is simply to strive for the Creating column of the Mastery group that will look like the following. Rule one—design cultural adaptation into the ESN, rule two—develop methods to improve networking, rule three—validate interpersonal connections, rule four—integrate leadership into bottom-up problem solving, and rule five—develop a sustainability plan for role models. Rule Six is already at the top of the scale.

The Intellipedia assessment by the rubric results in a score of 22 out of 36. An improvement approach to Intellipedia will look like the following. Rule one—examine the pace of culture adaptation, rule two—categorize the degree of connectedness, rule three—attribute value to connecting people, rule four—develop a process to streamline solution support, and rule five—develop a sustainability plan for role models. Like Peer-to-Patent, Intellipedia is at the top of the scale for rule six.

The average scores across the cases for each of the rules are not particularly illustrative. The average score for Rule One is 4, Rule Two is 4.3, Rule Three is 4.3, Rule Four is 3.3, Rule Five is 4, and Rule Six is 4.6. All the rules are between 2 and 6 points. The averages are between 3 and 5. This information is not nearly as helpful as the individual points for each rule for each case and then the cumulative score of the rules for each case.

Obviously, it is a strategic approach to improving ESNs. Further work in this area would involve developing operational and tactical approaches to each activity for each rule. An example of an operational approach could be to involve the fusion center community in collaboration with the National Fusion Center Association to leverage their analyst cadre to populate the HSE ESN. This option warrants further research on the integration of the fusion center community using an ESN.

Another application of the rubric is to be used for development of new ESNs. In this case, a wiki intended to serve as an ESN for the HSE with the ultimate goal of developing a BoK. The rubric serves to assist setting objectives based on the rules. The following illustrate an application of the rubric to establish objectives for the HSE BoK.

Rule One—Allow cultural change over time. Using the Mastering Group and the Creating column (six points), the objective would be, "Design cultural adaptation into the ESN." The planning team could then apply operational detail to meet that objective. For example, they could implement a semi-annual evaluation of participant engagement and then address any deficiencies.

Rule Two—Create opportunities for people to get to know one other. Using the Mastering Group and the Creating column (six points), the objective would be, "Develop methods to improve networking." The planning team could apply the operational detail. For example, they could schedule out-of-ESN social events for users to meet outside of the ESN. A national conference would be an option. The planning team could go so far as to offer free airfare and lodging to top contributors in exchange for presentations on their best practices. This approach also meets an objective of Rule Six—Consistently reward knowledge sharing behavior, at the Mastering Group and Creating column (six points)

level by “generating a culture of support for knowledge sharing behavior.” While not necessarily part of the design of the rubric, the mutual supporting qualities of the rules adds rigor to the process.

Rule Three—Focus on connecting people vice capturing content. The objective of using the Mastering Group and the Creating column is to “validate interpersonal connections.” This level of maturity about this rule focuses on the prioritization of interconnectedness over the sheer volume of content. The greater the degree of connectedness within the ESN, the greater the quality of the information, and the greater the degree of dissemination across the HSE.

Rule Four—Top-down support of bottom-up solutions. The Mastering Group and the Creating column states, “integrate leadership into bottom-up problem solving.” This maturity level shows the highest level of leadership involvement in support of solutions generated from the lower levels. An additional function of this level of maturity is an additional level of connectedness within the operational function of the ESN.

Rule Five—Provide positive role models wherever possible. The Mastering Group and Creating column for this rule states, “develop a sustainability plan for role models.” Mentorship over time of role models is a significant component of a mature ESN. This behavior also has a substantial impact on the culture, as traditions and norms are established and sustained when role models are held in high regard.

This approach to operational analysis addresses fundamental shortcomings of a wide variety of ESNs to include Wikipedia. It is also shown to be an effective guide to the creation of an ESN. It is suggested this approach could be used to address the demands for an effective HSE ESN.

The next chapter summarizes the premise of this thesis, the rules and the rubric, and the results of the application of the rules and the rubric to three cases.

# VI. CONCLUSION

This thesis has established the continued demand for improved information sharing by lawmakers and policymakers. Attempts have been made but a common HS-centric information-sharing platform still does not exist. The HSE is far larger than just the federal agencies or just LE or just the U.S. IC. The HSE spans across all levels and most disciplines of the government and includes the private sector as well.

The threats to the homeland continue to diversify and increase in complexity, which reinforces the need for increased connectedness across the HSE. Another consideration related to the HSE is the need for a BoK to reinforce HS as a discipline. Despite these demands, and the absence of a comprehensive platform for well over a decade, senior leadership across the HSE has not provided or recommended a viable approach. This thesis has attempted to address this need.

The literature related to this problem illustrates the persistent demand for getting "the right information to the right people at the right time," while not naming a specific approach to address this demand. There is no shortage of laws to include the PATRIOT Act, executive orders, strategic plans, and independent studies by GAO and the CRS directing agencies and organizations to find a way to attempt to meet these demands.

The continued demands and the associated inadequate attempts are beginning to result in a kind of information-sharing apathy from all the participants. This apathy is concerning because most likely it can revitalize the mentality of "need to know" at the expense of "need to share." This mentality could reasonably result in information blindness prior to the next significant HS incident.

This thesis looks to the concept of collective intelligence as an approach to connecting the HSE. This well-established approach to gathering information through the use of crowdsourcing could be an effective approach. By decentralizing the sources of information, and making that information available across the HSE, has a high probability of success. Basing this process on an ESN could bring necessary structure to this approach. This thesis has used a wiki as a viable ESN option.

This theory to unify the HSE will need some rigor to be accepted as a viable option by legislators and policymakers to allocate additional resources, and this thesis proposes a set of rules and a rubric based on well-established knowledge management and assessment research. The rules are (1) allow cultural change over time, (2) create opportunities for people to get to know one another, (3) focus on connecting people vice capturing content, (4) provide top-down support of bottom-up solutions, (5) serve as positive role models wherever possible, and (6) consistently reward knowledge sharing behavior.

The rules in and of themselves are not enough to provide sufficient guidance to the assessment or establishment of an ESN. The rules also require a rubric to serve as a guide for ESN planners to improve existing and create new ESNs. The ESN rubric employs Bloom's Taxonomy as a guide to assessing the maturity of an ESN. For each rule, the rubric applies the six gradations on Bloom's Taxonomy: remembering, understanding, applying, analyzing, evaluating, and creating along with a point system so that the ESN can receive a score for each rule, as well as a cumulative score.

Three ESNs served as case studies to validate this approach. All the ESNs are wikis and they are the ubiquitous Wikipedia, the USPTO's Peer-to-Patent and the DNI's Intellipedia. The background of the cases was discussed and then the rubric was applied to each of them that resulted in a maturity score for each of them. Wikipedia scored the highest followed by Intellipedia and then Peer-to-Patent.

These cases demonstrated the applicability and validity of the rubric. A more important application of the rubric is to serve as a planning tool for a potential HSE ESN, especially if the ESN employs a wiki. The planning team can balance the rubric against available resources to have a good sense of the initial maturity of the HSE ESN, as well as providing a path to achieve maximum maturity as additional resources become available.

The nature of the content of the HSE ESN could pose some security concerns. It is recommended the HSE ESN reside on a federal network and be classified at the *For Official Use Only* (FOUO) level. This level will meet the needs of the broadest

distribution and access while providing the necessary level of security for the information provided. A classified version of the ESN is really unnecessary. The sharing of information at the classified level is sufficiently addressed by the classified versions of Intellipedia.

The most recent publically available usage statistics show the top-secret version of Intellipedia has the most activity with 255,402 registered users, 113,379 pages, 290 million views, and 6.2 million edits. The secret version is next with 214,801 registered users, 107,349 pages, 246 million views, and 3.4 million edits. The unclassified version of Intellipedia is the least utilized of the three with 127,294 registered users, 48,274 pages, 94 million views, and 1.4 million edits.[231]

The HSE is composed of members from across all levels and many disciplines of government. It goes beyond LE and intelligence. It includes emergency management, public works, transportation, and planning divisions when addressing infrastructure protection. It includes public health agencies and non-governmental organizations, as well as hospitals and clinics when addressing pandemics. When discussing cybersecurity from a preventative perspective, the entirety of the HSE is involved. Virtually all the people involved in these areas do not have and have no need for a Secret or Top Secret security clearance.

The vast majority of useful information is at the FOUO level and the cost of trying to grant the entire HSE access would be staggering. A Federation of American Scientists report on security clearances determined the average cost of a Secret clearance at $241 and a Top Secret clearance at $3,959.[232] This price could cost the federal government tens of millions of dollars with no real benefit. Those who have a verifiable "need to know" tend to be connected to their federal partners and have the clearance necessary.

---

[231] Smathers, "Intellipedia Usage Statistics."

[232] Federation of American Scientists, S*uitability and Security Processes Review—Report to the President* (Washington, DC: Federation of American Scientists, 2014), 3, http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf.

The purpose of the BoK that would be the HSE ESN is to connect the lesser-known members of the HSE that have and can benefit from access to valuable unclassified information to other members of the HSE to include the LE and ICs.

This thesis has made possible significant improvements in the information-sharing process across the HSE by creating a simple and actionable assessment methodology. This process will hopefully keep the HSE engaged in the pursuit of optimal connectedness to avert or at least effectively respond to the wide range of threats facing the homeland.

It was not the intent of this thesis to solve this challenge completely, and as such, a plan to implement an HSE-wide ESN is beyond the scope. It is worthwhile to mention some implementation considerations for the ESN beyond what the rules and the rubric have to offer. Optimally, the broad nature of the community involved will require extensive support from the executive and legislative branches. Passing legislation mandating a HSE-centric ESN and appropriating the associated funding would be one of the most important first steps.

The incredibly collaborative nature of the HSE ESN would seem to most naturally fit within the DHS although there does not seem to be a single entity that could manage the administration of such a collaborative platform. Instead, the DHS should create a Joint Information-sharing Task Force (JISTF) comprised of a rotating staff from all the components within the DHS and across the HSE. Participants in the JISTF should reflect the HSE itself and be composed of multidisciplinary federal (to include legislative, as well as executive branch entities), SLTT government representatives, as well as the private sector.

Another option for implementing the HSE ESN would be for the JISTF to adopt the unclassified version of Intellipedia. It would need to be remodeled, and many of the openness policies would need to be refined using the rules and the rubric and significant effort would need to be exerted to increase participation dramatically for this approach to be successful.

This approach or a similar version goes a long way in addressing some of the most vexing problems facing the persistent challenges to HS information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


American Hospital Association. “Fast Facts on U.S. Hospitals.” January 2, 2014. http://www.aha.org/research/rc/stat-studies/fast-facts.shtml.

Andrus, D. Calvin. “The Wiki and the Blog.” *Intelligence* 49, no. 3 (2005): 1–30.

Ayers, Phoebe, Charles Matthews, and Ben Yates. *How Wikipedia Works: And How You Can Be a Part of It*. San Francisco: No Starch Press, 2008. Kindle edition.

Best, Richard A. Jr. *Intelligence Information: Need-to-Know vs. Need-to-Share*. (CRS Report No. R41848). Washington, DC: Congressional Research Service, 2011. https://www.fas.org/sgp/crs/intel/R41848.pdf.

Best, Richard A. Jr. *Sharing Law Enforcement and Intelligence Information: The Congressional Role*. (CRS Order Code RL33873). Washington, DC: Congressional Research Service, 2007.

Bonnett, Travis. “In Defense of Wikipedia: An Editorial.” American Library Association. May 2010. http://www.ala.org/nmrt/news/footnotes/may2010/in_defense_of_wikipedia_bonnett.

Brabham, Daren C. *Crowdsourcing*. Cambridge, MA: The MIT Press, 2013. Kindle edition.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. London: Penguin Group USA, 2006. Kindle edition.

Brown, Harold, and Warren B. Rudman. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Darby, PA: Diane Publishing, 1996.

Bush, George W. “Executive Order 13388.” Federation of American Scientists, October 25, 2005. http://www.fas.org/irp/offdocs/eo/eo-13388.htm.

Center on Standards and Assessment Design, The. “Assessment Design Toolkit.” Accessed October 17, 2016. http://www.csai-online.org/spotlight/assessment-design-toolkit#repurpose the toolkit.

———. “Part 1—Key Concepts.” Accessed October 17, 2016. http://www.csai-online.org/spotlight/part-i-key-concepts#part-2.

Central Intelligence Agency. “Intellipedia Gurus Win 2009 Homeland Security Medal.” April 30, 2013. https://www.cia.gov/news-information/featured-story-archive/intellipedia-homeland-security-medal.html.

Clapper, James C. *Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence 2016.

Dalkir, Kimiz, and Jay Liebowitz. *Knowledge Management in Theory and Practice*. Cambridge, MA: The MIT Press, 2011. Kindle edition.

Department of Justice, Justice Information Sharing. "The Implementing Recommendations of the 9/11 Commission Act of 2007." Accessed July 24, 2014. https://it.ojp.gov/default.aspx?page=1283.

———. "The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)." Accessed July 24, 2014. https://it.ojp.gov/default.aspx?page=1282.

Dixon, Nancy M., and Laura A. McNamara. *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*. Arlington, VA: DIA Knowledge Laboratory, 2008.

Doyle, Charles. *The USA PATRIOT Act: A Legal Analysis.* (CRS Order Code RL31377). Washington, DC: Congressional Research Service, 2002.

Ebersbach, Anja, Markus Glaser, Richard Heigl, and Alexander Warta. *Wiki: Web Collaboration*. Berlin: Springer Science & Business Media, 2008.

Federation of American Scientists. S*uitability and Security Processes Review—Report to the President*. Washington, DC: Federation of American Scientists, 2014. http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf.

Fingar, Thomas. "Intelligence Reform [Rush Transcript; Federal News Service]." Council on Foreign Relations. March 18, 2008. http://www.cfr.org/intelligence/intelligence-reform-rush-transcript-federal-news-service/p15754.

Graham, Bob, and Richard C. Shelby. *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*. Washington, DC: Senate Intelligence Committee, 2002. http://www.intelligence.senate.gov/pdfs/1071086v2.pdf.

Gruber, Hans-Georg. "Does Organizational Culture Affect the Sharing of Knowledge, The Case of a Department in a High Technology Company." Master's thesis, Carleton University, 2000.

International Association of Chiefs of Police. *Strategic Plan*. Alexandria, VA: International Association of Chiefs of Police, 2010. http://www.iacp.org/portals/0/pdfs/IACPStrategicPlan.pdf.

International Association of Fire Chiefs. "EMR-ISAC: A Critical Information-Sharing Tool." October 15, 2011. http://www.iafc.org/MemberCenter/OnSceneArticle.cfm?ItemNumber=5184.

International Association of Law Enforcement Intelligence Analysts. “Mission.” Accessed November 20, 2016. http://www.ialeia.org/about-us/mission.html.

Jackson, Joab. “Intellipedia Suffers Midlife Crisis.” *Government Computer News*, February 18, 2009. http://gcn.com/Articles/2009/02/18/Intellipedia.aspx.

Jemielniak, Dariusz. *Common Knowledge?: An Ethnography of Wikipedia*. Stanford, CA: Stanford University Press, 2014. Kindle edition.

Karter, Michael J. Jr., and Gary P. Stein. “U.S. Fire Department Profile.” National Fire Protection Association, October 1, 2013. http://www.nfpa.org/research/reports-and-statistics/the-fire-service/administration/us-fire-department-profile.

Keyes, Jessica. *Enterprise 2.0: Social Networking Tools to Transform Your Organization*. Boca Raton, FL: CRC Press, 2012.

Kim, Eugene Eric. “Intellipedia Shovel.” Eugene Eric Kim Comments, September 27, 2006. http://eekim.com/blog/2006/09/intellipedia-shovel/.

Larence, Eileen. *Information-Sharing—DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts*. (GAO-12-809). Washington, DC: U.S. Government Accountability Office, 2012. http://www.gao.gov/assets/650/648475.pdf.

Larence, Eileen R. *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*. (GAO-12-144T). Washington, DC: Government Accountability Office, 2011. http://www.gao.gov/assets/590/585711.pdf.

Leistner, Frank. *Connecting Organizational Silos: Taking Knowledge Flow Management to the Next Level with Social Media*. Hoboken, NJ: Wiley, 2012. Kindle edition.

Leuf, Bo, and Ward Cunningham. *The Wiki Way: Quick Collaboration on the Web*. Boston, MA: Addison-Wesley Professional, 2001.

Library of Congress. “Bill Summary & Status 107th Congress (2001–2002) H.R. 5005 CRS Summary.” Accessed June 26, 2014. http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05005:@@@D&summ2=m&.

Markle. “Markle Task Force on National Security.” Accessed December 5, 2016. https://www.markle.org/national-security/markle-task-force-national-security.

———. “Meeting the Threat of Terrorism: Culture Change.” September 1, 2009. http://www.markle.org/publications/499-meeting-threat-terrorism-culture-change.

———. “Nation At Risk: Policy Makers Need Better Information to Protect the Country.” March 1, 2009. http://www.markle.org/publications/487-nation-risk-policy-makers-need-better-information-protect-country.

———. “National Security.” Accessed December 5, 2016. https://www.markle.org/national-security.

Masunaga, Yoshifumi, Yoshiyuki Shoji, and Kazunari Ito. “A Wiki-based Collective Intelligence Approach to Formulate a Body of Knowledge (BOK) for a New Discipline.” In *Proceedings of the 6th International Symposium on Wikis and Open Collaboration*, art. 11. Gdansk, Poland—July 07–09, 2010, New York: ACM, 2010.

McConnel, James. *Director of National Intelligence Strategic Vision 2015*. Maxwell AFB, AL: The Air University, 2014. http://www.au.af.mil/au/awc/awcgate/dni/vision_2015_july08.pdf.

Mihm, Christopher J. *Key Considerations for Implementing Interagency Collaborative Mechanism*. (GAO-12-1022). Washington, DC: Government Accountability Office, 2012. http://www.gao.gov/assets/650/648934.pdf.

National Archives and Records Administration. “FAQ’s About Executive Orders.” Accessed August 13, 2014. http://www.archives.gov/federal-register/executive-orders/about.html#orders.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office, 2011.

National Fusion Center Association. “Home.” Accessed November 20, 2016. https://nfcausa.org/default.aspx/MenuItemID/135/MenuGroup/Public Home.htm.

Noveck, Beth Simone. *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*. Washington, DC: Brookings Institution Press, 2009. Kindle edition.

Office of the Director of National Intelligence. *Strategic Intent for Information-sharing*. Washington, DC: Office of the Director of National Intelligence, 2011. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/11152526_strategic_intent_info_sharing.pdf.

Powner, David A. *Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives*. (GAO-07-455). Washington, DC: Government Accountability Office, 2007. http://www.gao.gov/assets/260/259384.pdf.

Reagle, Joseph M., and Lawrence Lessig. *Good Faith Collaboration: The Culture of Wikipedia*. Cambridge, MA: MIT Press, 2012. Kindle edition.

Reaves, Brian A. “Bureau of Justice Statistics (BJS).” Census of State and Local Law Enforcement Agencies, July 26, 2011. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2216.

Reese, Shawn. *Defining Homeland Security: Analysis and Congressional Considerations*. (CRS Report No. R42462). Washington, DC: U.S. Congressional Research Service, 2013. http://www.fas.org/sgp/crs/homesec/R42462.pdf.

Salminen, Juho. *Collective Intelligence in Humans: A Literature Review*. Ithaca, NY: Cornell University Library, 2012. https://arxiv.org/abs/1204.3401.

Schiff, Stacy. “Know It All.” *The New Yorker*, July 31, 2006. http://www.newyorker.com/magazine/2006/07/31/know-it-all.

Smathers, Jason. “Intellipedia Usage Statistics.” MuckRock, January 28, 2014. https://www.muckrock.com/foi/united-states-of-america-10/intellipedia-usage-statistics-10058/#file-16141.

Surowiecki, James. *The Wisdom of Crowds*. New York: Knopf Doubleday Publishing Group, 2005. Kindle edition.

Theohary, Catherine A., and John Rollins. *Terrorist Use of the Internet: Information Operations in Cyberspace*. (CRS Report No. R41674). Washington, DC: Congressional Research Service, 2011. http://www.fas.org/sgp/crs/terror/R41674.pdf.

U.S. Department of Homeland Security. *2014 Quadrennial Homeland Security Review*. Washington, DC: U.S. Department of Homeland Security, 2014. http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

———. *Intelligence Information-sharing Final Report and Recommendations*. Washington, DC: U.S. Department of Homeland Security, 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

———. *Office of Intelligence and Analysis Strategic Plan*. Washington, DC: U.S. Department of Homeland Security, 2011. http://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors’ Characteristics*. (GAO-07-39). Washington, DC: U.S. Government Accountability Office, 2006. http://www.gao.gov/products/GAO-07-39.

U.S. House of Representatives. *Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security*. Washington, DC: U.S. House of Representatives, 2013. http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-DavisE-20130509.pdf.

U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence. *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*. Washington, DC: U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, 2002. http://fas.org/irp/congress/2002_rpt/911rept.pdf.

United States Patent and Trademark Office. "About Us." February 12, 2015. http://www.uspto.gov/about-us.

Washington State University. *Guide to Rating Critical & Integrative Thinking Washington, Fall 2006.* Pullman, WA: Washington State University, 2006. http://www.cpcc.edu/learningcollege/learning-outcomes/rubrics/WST_Rubric.pdf.

Weiss, N. Eric. *Legislation to Facilitate Cybersecurity Information-sharing: Economic Analysis*. (CRS Report No. R43821). Washington, DC: Congressional Research Service, 2014. http://www.fas.org/sgp/crs/misc/R43821.pdf.

White House. *2010 National Security Strategy*. Washington, DC: White House, 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

———. *2015 National Security Strategy*. Washington, DC: White House, 2015. http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

———. "Executive Order -- Promoting Private Sector Cybersecurity Information-sharing." February 13, 2015. http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing.

———. *National Strategy for Information-sharing and Safeguarding.* Washington, DC: White House, 2012.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California