Open-Source Approach to NIPP Risk Assessment Implementation

C. David Binning, P.E. and Jenyl L. Meszaros

January 2014

ABSTRACT

The National Infrastructure Protection Plan (NIPP) was put into place in 2013 to protect the critical infrastructure of the United States. The critical infrastructure spans 18 sectors including banking, energy, water, transportation, and a wide variety of other fields. The NIPP emphasizes the high priority that all sectors now must place on risk assessment and operational sustainability. This paper discusses an approach for the development of an open source software for these sectors to effectively communicate, develop, and implement risk management practices. There are many advantages to providing an open source approach to risk assessment and management including an ability to quickly develop sector specific programs to assist in risk analysis. Risk assessment and sustainability development, based on NIPP protocol approach is proposed to support individual sector development as well as help facilitate the analysis of interdependencies between sectors. Development of sector-specific applications by standards-setting organizations is suggested as a means to guide, vet, and expand the knowledge-base of those charged with the operation and safeguarding of our national critical infrastructure.

Table of Contents

Introduction

Over the past decade the U.S. has experienced a major terrorist attack on domestic soil, as well as numerous significant natural disasters. The occurrence of these events, as well as the continued threat of such events, has made clear the importance of protecting our Nation's critical infrastructure. Critical infrastructure is defined by federal law as "systems and assets, whether physical or virtual, so vital to the United States (U.S.) that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Critical Infrastructure Protection 2009). The 18 critical infrastructure sectors identified by the Department of Homeland Security (DHS) are as follows:

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Servicesassets
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

The Homeland Security Act of 2002 charged DHS with primary responsibility for developing a comprehensive national plan to secure critical infrastructure and for recommending necessary measures to protect the critical infrastructure and key resources (CIKR) of the U.S. This comprehensive plan is the National Infrastructure Protection Plan (NIPP), which was published by DHS in June 2006 (Critical Infrastructure 2010). The NIPP provides the unifying structure that integrates a wide range of protective security efforts into a single national program. The cornerstone of the NIPP is its risk and resilience analysis and management framework that establishes the processes for combining consequence, vulnerability, threat, and resilience information to produce assessments of national or sector risk. This framework was based on a risk analysis approach developed by the American Society of Mechanical Engineers (ASME)-Innovative Technologies Institute (ITI) known as Risk Analysis and Management for Critical Asset Protection (RAMCAPSM) (National InfrastructureProtection Plan 2009).

In 2003, Homeland Security Presidential Directive 7 (HSPD-7) designated a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programs and activities within each sector. Each of the SSAs developed a Sector-Specific Plan (SSP) that details the application of the NIPP framework to the unique characteristics of their sector (Critical Infrastructure 2010). In addition, through the development of sector-specific guidance documents by ASME-ITI, the RAMCAPSM approach has been tailored to the technologies, issues, and cultures of several of the sectors (ASME-ITI 2009). As a result of this sector-specific guidance, several industries have developed sector-specific standards and tools for applying the NIPP/RAMCAPTM methodology. For example, the American Water Works Association (AWWA) and ASME developed the "RAMCAP® Standard for Risk and Resilience Management of Water and Wastewater Systems" (AWWA/ASME-ITI 2010), which was published in July 2010 and is an approved American National Standards Institute (ANSI) standard (J-100).

PROBLEM STATEMENT

Since the publication of the NIPP and the SSPs, agencies and organizations nationwide have been working to apply the frameworks and to develop tools to assist them in their efforts; however, even with the NIPP and the SSPs at the heart of these efforts, the J-100 water and wastewater standard is the only standard to be developed and adopted for applying the NIPP risk analysis and management framework. Further, while there have been a number of sector-specific tools developed to assist agencies in their efforts, it is not clear whether these tools are compliant with the NIPP risk analysis and management framework.   As an example, the water and wastewater sector, a leader in infrastructure risk assessment, made an attempt to adapt two of the sector's existing risk assessment tools owned by the Environmental Protection Agency (EPA) and the Department of Homeland Security (DHS) to be consistent with the J-100 ANSI standard developed specifically for the sector; however, a recent gap analysis of these software tools found that they fall short of being compliant with the standard.

The water and wastewater sector is an example of how it is not easy to adapt software tools to a standard, particularly since the standard is continually being updated. The problem then is a lack of approved, standardized tools that can evolve as the frameworks and standards are updated. What is needed is a more dynamic approach to developing and maintaining standards-compliant tools that keep pace with the rapidly changing frameworks and standards. An alternative approach that would afford the rapid development of standards-compliant software tools is open source software development.

"Open source software" refers to a software development process that takes place in a collaborative, peer reviewed, transparent environment with the objective of developing a higher quality, more reliable, more flexible, lower cost end product as compared to traditional, centrally-developed proprietary software tools. While "open source" is currently a buzz phrase used commonly when referring to software, it is not always used in the true sense of the phrase. The Open Source Initiative (OSI) serves as a standards body, maintaining the Open Source Definition, which OSI uses to determine whether or not a software license can be considered open source. Open source does not just mean access to the source code – the distribution terms of an open source program must comply with the ten criteria laid out in the Open Source Definition (Perens 1999). Because the term "open source" cannot be trademarked, there is little OSI can do to prevent improper usage of the term; however, OSI created a certification mark, "OSI Certified," that is used on software that is being distributed under a license that conforms to the Open Source Definition (OSI Certification Mark and Program 2007). It is the OSI Approved License trademark and program that creates a nexus of trust around which developers, users, corporations and governments can organize open source cooperation (Open Source Initiative 2011).

OBJECTIVES

The objectives of this paper are twofold. The first objective is to make the case for and to suggest an open-source framework for the development and maintenance of standards and standards-compliant software that can keep pace with the dynamically changing risk assessment methodologies and standards. The development of an approved national standard compliant with the NIPP risk analysis and management framework and the hosting of a nationwide repository for open-source software are major efforts that require the support and guidance of one or more well-respected, national organizations. The second objective of this paper is to identify and evaluate agencies and organizations that could assume the role of standards developer and that could serve as a nationwide repository for the development of open source software tools.

AN OPEN SOURCE APPROACH TO CRITICAL INFRASTRUCTURE RISK ASSESSMENT AND MANAGEMENT

The first objective of this paper is to make the case for and to suggest an open-source framework for the development and maintenance of standards and standards-compliant software that can keep pace with the dynamically changing risk assessment methodologies and standards as opposed to developing closed-source software by individual organizations/companies that cannot be easily adapted to these rapid changes – literally thinking outside of the proverbial black box.

A state of the practice review revealed that there are a number of tools already available for assessing the vulnerability of critical infrastructure assets across various sectors, including the following:

- **Food and Agriculture Criticality Assessment Tool (FASCAT) –** The Food and Agriculture Government Coordinating Council (GCC) partnered with the University of Minnesota's National Center for Food Protection and Defense (NCFPD) to develop the FASCAT (FASCAT 2011). FASCAT is a web-based software tool that applies the NIPP framework for assessing hazards and the criticality of supply chain nodes, systems, and sub-systems to assist states in determining and documenting their most critical food and agriculture infrastructure (National Infrastructure Protection Plan 2008). FASCAT provides a means to identify key state commodity chains or food distribution systems, a consistent method to prioritize state or private sector vulnerabilities, and possible protective strategy development. It documents and characterizes a state's food and agriculture sector risk profile, as well as an effective response to future DHS national data calls for information on critical food and agriculture infrastructure.

- **CCPS® SVA (Center for Chemical Process Safety Security Vulnerability Assessment)** for fixed chemical sites (Errata to guidelines 2002).

- **API/NPRA (American Petroleum Institute/National Petrochemical & Refiners Association) SVA –**The API and NPRA developed an SVA to assist the petroleum and petrochemical industry in understanding security vulnerability assessment and in conducting SVAs. This approach consists of six steps that include understanding what critical assets need to be secured, identifying and characterizing threats against those assets, identifying potential security vulnerabilities, determining the likelihood of a successful event and the consequences of an event if it were to occur, ranking the risk of the event occurring, and identifying and evaluating risk mitigation options (API NPRA SVA, 2007).

- **SOCMA (Society of Chemical Manufactures and Affiliates) SVA model and manual –** The SOCMA SVA model and manual are computer-based tools that incorporate the elements of inherent hazards, attractiveness, potential consequences, and existing security measures in a tiered screening process. The tool provides chemical facilities with a mechanism to allow flexibility and efficiency in site vulnerability analysis (SOCMA's 2011).

- **Vulnerability Identification Self-Assessment Tool (ViSAT) –** Various online modules were launched by DHS in 2005 for commercial facility managers to raise the level of security at convention centers, arenas, stadiums, race tracks, performing arts centers, and shopping centers (Commercial Facilities Snapshot 2008).

- **Risk Self-Assessment Tool (RSAT) for Stadiums and Arenas** is a secure, web-based application designed to assist managers of stadiums and arenas with the identification and management of security vulnerabilities to reduce risk to their facilities. The RSAT application was developed in partnership with the Office of Infrastructure Protection's SSA Executive Management Office (EMO) and the Infrastructure Information Collection Division. The RSAT application uses facility input in combination with threat and consequence estimates to conduct a comprehensive risk assessment and provides users with options for consideration to improve the security posture of their facility (Risk Self-Assessment 2009).
- **Dams Sector Analysis Tool (DSAT) –** Developed by DHS, DSAT is a "web-based tool providing Dams Sector partners with secure access to different modules and applications covering a wide range of analytical capabilities" (ASDSO eNews 2011).
- **Department of Homeland Security Vulnerability Identification Self-Assessment Tool-Transportation (DHS-VISAT-T) -** Developed by the Transportation Security Agency (TSA) as a user-friendly, flexible, web-based tool to support the unique characteristics of each transportation mode, while still providing a common framework from which analysis and trends can be identified. DHS-VISAT-T assists all modes of transportation asset owners/operators in developing a security plan and in performing a vulnerability assessment of their assets and is provided at no cost to transportation owner and operators. The tool captures a snapshot of the asset's baseline security posture and assists the stakeholder in conducting a vulnerability assessment and completing a comprehensive security plan. TSA has developed modules of the tool for maritime, mass transit, highway bridges, and rail passenger stations (TSA 2009).
- **Vulnerability Self Assessment Tool (VSAT™) -** The Vulnerability Self Assessment Tool (VSAT™) software was developed to support water and wastewater utility vulnerability assessments using a qualitative risk assessment methodology. VSAT™ software is available, free of charge, for wastewater utilities (VSATwastewater™), drinking water utilities (VSATwater™), and for utilities providing both services (VSATwater/wastewater™) (Vulnerability Assessments 2010).

While the risk analysis tools presented above exist for use by agencies and organizations, it is not clear whether the methodologies they use are consistent and compliant with the NIPP risk analysis and management framework, as a process for software compliance evaluation has yet to be formally developed or adopted. In addition, it appears that none of the tools have been developed in an open source environment, which limits the compliance assessment to a black box evaluation.

In a 2010 article in the ASCE Journal of Computing in Civil Engineering, Moffat and Laefer assert that a new software development paradigm is needed to update Hazard U.S. (HAZUS 2011) and propel it to the forefront of the next generation of disaster management software tools (Laefer 2010). HAZUS is a nationally applicable standardized methodology that uses Geographic Information Systems (GIS) technology and models to estimate physical, economic, and social impacts from earthquakes, floods, and hurricanes. Although HAZUS is distributed at no cost by FEMA, the program's functionality is restricted by an underlying commercial off-the-shelf (COTS) GIS. According to Moffat and Laefer, proprietary, stand alone, and single-user disaster management systems prevent efficient data gathering and sharing

capabilities and result in circumscribed utility and productivity. Their recommendation is to replace the proprietary, standalone desktop version of HAZUS with a three-tier, distributed architecture based on open source design and development principles (Laefer 2010).

APPLICATION AND BENEFITS OF OPEN SOURCE SOFTWARE WITHIN THE CRITICAL INFRASTRUCTURE SECTORS

While most of the risk analysis tools in existence today were not developed in an open source environment, agencies and organizations within many of the critical infrastructure sectors are beginning to recognize the benefits and embrace the idea of open source software. The following examples illustrate the benefits of the use of an open source software approach within several of the critical infrastructure sectors, albeit not all of the examples are necessarily applications of critical infrastructure risk assessment and protection.

Agriculture and Food

The Food and Agriculture Organization of the United Nations (FAO) recently moved to an open source server-side database standard. Key activities of the FAO include putting information within reach, sharing policy expertise, and bringing knowledge to the field. Over 200 database systems are used to collect, analyze, and disseminate knowledge and data that aid development of the member countries. Until now, almost all systems have been based on a proprietary database system, but FAO recognized that the inclusion of open source software solutions could help the Organization better accomplish its mandate and objectives (United Nations 2006).

Emergency Services

The Open Information Systems for Emergency Services (ISES) Project was created to help emergency response personnel meet their needs and responsibilities through the use of free, open source software and support materials. The Open ISES Project is working on creating training materials for basic Emergency Medical Technician (EMT), continuing medical education, hazardous materials, terrorism, management and leadership (Welcome to the Open ISES Project).

Energy

The Energy Sector Security Consortium (EnergySec) and Oregon State University's Open Source Lab (OSUOSL) have partnered to perform strategic research on the current use of open source software in the energy sector, especially within the area of cyber security, and to produce an inventory of the experienced companies and groups in this space. The aim of this research is to build up a significant body of knowledge regarding how and why energy companies and groups participate in open source, both as users and as contributors (New Study 2011).

Transportation

Transit

The Tri-County Metropolitan Transportation District of Oregon (TriMet), the transit agency serving the Portland area, is aggressively pushing open source for every software purchase and is increasingly selecting the open source option. Initially, the agency steadily integrated open source into smaller back-office functions. Beginning in 2007, the agency took a bigger step, swapping several closed source GIS products with open source alternatives. Using an open source application supported by a third-party developer gave TriMet more control over changes. TriMet's IT manager of GIS and location-based services commented that, before going with open source software, they could only cross their fingers that a feature request submitted to the software development company would be in the next release. The open source route has given them more control, especially when they have the money to support the development of the features they want (Opsahl 2011).

One open source application that TriMet's in-house programmers are developing for the agency's website is OpenTripPlanner, which plans trips for citizens by combining the various modes of public transportation, such as buses and trains, available in a district. Currently TriMet.org uses a trip planning system from a vendor, but the system does not combine various transportation modes. TriMet looked at a proprietary product used by another major transit agency, but found it to be too expensive. So TriMet's IT staff set out to establish a community for developing OpenTripPlanner. TriMet's IT manager was quoted as saying, "It's amazing. We have developers from all over the world who are contributing to this application, and the development cycle and the feature cycle is very, very fast" (Opsahl 2011).

Traffic Management

On October 20, 2010, the U.S. Department of Transportation's Intelligent Transportation Systems (ITS) Joint Program Office hosted a webinar on an open source alternative to deploying transportation management systems. Historically, acquiring a transportation management system has required a huge investment of capital and a long implementation timeframe. Often, the acquiring agency is beleaguered with nondisclosure agreements, is left with little or no software documentation, and is often forced to execute sole-source contracts in order to maintain the system. Additionally, the agency inherits COTS software and hardware components that require costly annual maintenance agreements. In this time of economic uncertainty, agencies need more transparency into the systems they acquire and a competitive and economic means of deploying and maintaining these systems. Most importantly, it is time for DOTs to reach out and collaborate on common solutions. In this webinar, two state agencies—the California DOT (Caltrans) and the Minnesota DOT (Mn/DOT)—discussed and demonstrated how they derived individual and mutual benefits using the open source Intelligent Roadway Information System (IRIS) Advanced Transportation Management System (ATMS) (Open Source Alternative 2010).

Water

In a recent paper, Tabor, et al., examined the application of OpenFOAM to urban water management modeling. Specifically, they examined the quality of the technical results and the value added to the process through adoption of open source software solutions. In the past, most Computation Fluid Dynamics (CFD) calculations have been performed using one of a number of commercial CFD codes. Recently, alternative codes operating under the open source licensing model have become available, such as OpenFOAM. These open source codes have a number of advantages - the level of usage is not dictated by licensing costs, and the availability of the code promotes modification, verification, and code sharing (Tabor et al. 2011).

CANARY Event Detection Software is an open source software tool developed by Sandia National Laboratories in partnership with the Environmental Protection Agency (EPA). The software tells utility operators within minutes whether something is wrong with their water, giving them time to warn and protect the public. Use of the software is also helping to improve water quality by giving utility managers more comprehensive real-time data about changes in their water (Sandia 2011).

FRAMEWORK FOR THE CONTINUED DEVELOPMENT AND MAINTENANCE OF STANDARDS AND OPEN SOURCE SOFTWARE TOOLS FOR THE ASSESSMENT OF CRITICAL INFRASTRUCTURE

This section of the paper presents and describes a suggested framework for the continued development and maintenance of standards and the development of open source software tools for risk assessment and management of critical infrastructure. The suggested framework is illustrated in figure 1.

The diagram represents the NIPP community and its progress towards developing open source tools that are compliant with the NIPP risk analysis and management framework. The left side of the diagram represents the "foundation" of the development of standards and open source software tools to support critical infrastructure risk assessment and management. On the foundation side, engineering professional organizations lead the development and maintenance of standards and set requirement priorities for software development that are standards-compliant. Open source software code is developed by the IT community and deposited into an open source repository. On the foundation side, the software development process is dynamic, open for collaboration, and driven by a steering committee. Sector leaders can deposit and pull from the repository based on established guidelines. This process continues until the software become stable enough to transition to the "derivatives" side of the process.

The "derivatives" side of the open source software develop process is shown on the right side of the diagram. In this phase of software developing, the software goes through a more robust design, testing, and certification process. The code is tested from a software perspective and the software is then certified by the engineering community that it is compliant with the standards and that it meets engineering requirements. While the software is made available to users at no cost, a fee based structure is applied to pay for software support that comes with each version of the software.

The yellow bars are for illustration only and represent each of the 18 critical infrastructure sectors and their eventual progress towards the development, design, testing, and certification of open source, standards-compliant software.

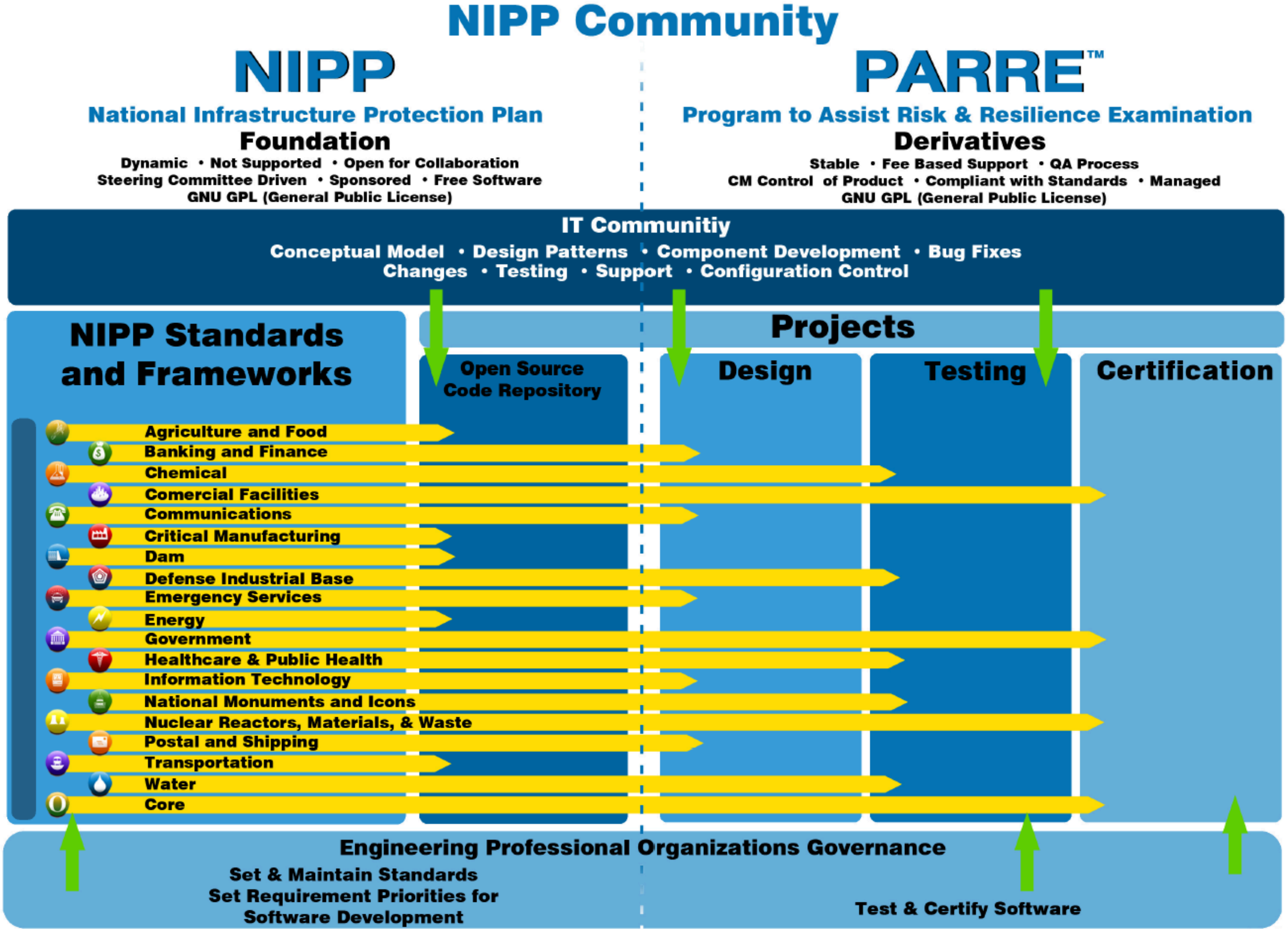
NIPP Community
NIPP
National Infrastructure Protection Plan
Foundation
Dynamic • Not Supported • Open for Collaboration
Steering Committee Driven • Sponsored • Free Software
GNU GPL (General Public License)
PARRE™
Program to Assist Risk & Resilience Examination
Derivatives
Stable • Fee Based Support • QA Process
CM Control of Product • Compliant with Standards • Managed
GNU GPL (General Public License)
IT Communitiy
Conceptual Model • Design Patterns • Component Development • Bug Fixes
Changes • Testing • Support • Configuration Control
NIPP Standards and Frameworks
Projects
Open Source Code Repository
Design
Testing
Certification
Agriculture and Food
Banking and Finance
Chemical
Comercial Facilities
Communications
Critical Manufacturing
Dam
Defense Industrial Base
Emergency Services
Energy
Government
Healthcare & Public Health
Information Technology
National Monuments and Icons
Nuclear Reactors, Materials, & Waste
Postal and Shipping
Transportation
Water
Core
Engineering Professional Organizations Governance
Set & Maintain Standards
Set Requirement Priorities for Software Development
Test & Certify Software

Figure 1. The NIPP Community Open Source Model

DEVELOPMENT AND MAINTENANCE OF NATIONAL STANDARDS COMPLIANT WITH THE NIPP RISK MANAGEMENT FRAMEWORK

There are numerous agencies and organizations that could assume the role of developing and maintaining a national standard for assessing and managing critical infrastructure risk, as well as the development and maintenance of sector-specific standards, and that could serve as a national repository for open source software code.

As this is a major undertaking, this section of the paper presents the characteristics that are considered key for an organization to lead these efforts. A list of organizations possessing these characteristics is also presented as a starting point for identifying organizations that are well-positioned to lead these efforts.

FRAMEWORK FOR THE CONTINUED DEVELOPMENT AND MAINTENANCE OF STANDARDS AND OPEN SOURCE SOFTWARE TOOLS FOR THE ASSESSMENT OF CRITICAL INFRASTRUCTURE

As has been discussed, while the NIPP risk analysis and management framework has been used by agencies and organizations nationwide, the methodology has yet to be developed into a national standard. The recent occurrences, and continued threat, of terrorist attacks and natural disasters in the U.S. has made clear the importance of developing national standards for assessing the risk and resilience of the Nation's critical infrastructures. To ensure that the risk assessment process is being conducted in a systematic, consistent manner and that the results can be directly compared, it is critical that a national standard be developed and approved. There is a need for an organization to assume this role and to lead the development of a national standard for assessing all-hazards risk and resilience.

In identifying an organization that might assume the role of developing and maintaining a national standard compliant with the NIPP risk management framework, the following characteristics are considered to be key:

- Must be within the domain of infrastructure protection.
- Must be a standards development organization (SDO).
- Must have an interested audience.
- Must be willing to assume the role as standard developer.

Based on an assessment of potential organizations, the American Society of Civil Engineers (ASCE) is considered to be a front-runner for the role of developing and maintaining as a national standard for infrastructure risk assessment. ASCE was established over 150 years ago. It represents more than 140,000 members of the civil engineering profession worldwide and is America's oldest national engineering society (About ASCE 2011). One of ASCE's three strategic priorities is to propose practical solutions to improve America's neglected infrastructure. In December 2008, ASCE sponsored an industry summit to identify content for a guidance document outlining key attributes required for successful, safe, resilient, and sustainable critical infrastructure systems. The summit fostered meaningful discussions and insights from experts with wide-ranging roles in critical infrastructure (Guiding Principles 2008). In addition, ASCE is an accredited SDO by the American National Standards Institute (ANSI) and has developed more than 60 published ASCE Standards that provide technical guidelines for promoting safety, reliability, productivity and efficiency across all areas of civil engineering (Codes and Standards 2011).

IDENTIFICATION OF ORGANIZATIONS TO DEVELOP AND MAINTAIN A NATIONAL STANDARD COMPLIANT WITH THE NIPP RISK MANAGEMENT FRAMEWORK

While the NIPP presents a framework for assessing the overall vulnerability of critical infrastructure, sector-specific methodologies, in accordance with the SSPs, are needed to better manage the risk and resilience of the specific assets within each of the critical infrastructure sectors. As an example, the water and wastewater industry developed the J-100 ANSI standard for managing the risk and resilience of water and wastewater systems (AWWA/ASME-ITI 2010).

As with the development of an approved national standard for infrastructure risk assessment and management, organizations within each of the critical infrastructure sectors need to be identified to assume the role of developing and maintaining sector-specific standards for assessing all-hazards risk and resilience. Similar to the characteristics considered key for the lead organization in the development of an overall national standard, the following chara teristics are considered key in identifying organizations that might assume the role of developing and maintaining sector-specific standards for infrastructure risk assessment:

- Must be within the critical infrastructure domain (e.g., energy, transportation).
- Must be an SDO.
- Must have an interested audience.
- Must be willing to assume the role as standard developer.

The table below lists the critical infrastructure sectors as defined by DHS, as well as the designated federal SSA to lead protection and resilience-building programs and activities within each sector. Based on an assessment of organizations, the third column in the table lists potential organizations possessing the above characteristics that might serve the lead role in the development and maintenance of sector-specific standards.

Table 1. Potential Organizations to Develop Critical Infrastructure Sector-Specific Standards

Critical Infrastructure Sector	**Sector Specific Agency (SSA)**	**Potential Organizations to Develop Sector Specific Standards**
Agriculture and Food	Dept. of Agriculture Dept. of Health and Human Services	• American Society of Agricultural and Biological Engineers (ASABE) (ASABE 201) (1) • National Association of State Departments of Agriculture (NASDA) (2)
Banking and Finance	Dept. of the Treasury	• Consortium of Investment Banking Institution Standards (CIBIS)
Chemical	Dept. of Homeland Security – Office of Infrastructure Protection	• American Institute of Chemical Engineers (AIChE) (3) • American Petroleum Institute (API) (3)
Commercial Facilities	Dept. of Homeland Security – Office of Infrastructure Protection	• U.S. Chamber of Commerce
Communications	Dept. of Homeland Security – Office of Cyber Security & Communications	• Telecommunications Industry Association (TIA) • Cellular Telecommunications Industry Assoc.(CTIA) • Lucent Technologies
Critical Manufacturing	Dept. of Homeland Security – Office of Infrastructure Protection	• Society of Manufacturing Engineers (3) • Ford Motor Company • General Motors Company
Dams	Dept. of Homeland Security – Office of Infrastructure Protection	• American Society of Civil Engineers (ASCE)
Defense Industrial Base	Dept. of Defense	• National Association of Manufacturers (NAM)

Emergency Services	Dept. of Homeland Security – Office of Infrastructure Protection	• American Public Works Association (APWA) • National Fire Protection Association (NFPA) • International Assoc. of Chiefs of Police (IACP)(2) • International Assoc. of Emergency Managers (IAEM) (2) • International Association of Fire Chiefs (IAFC)(2) • National Assoc. of State EMS Officials (NASEMSO) (2) • National Emergency Management Association (2) • National Sheriffs Association (NSA) (2)
Energy	Dept. of Energy	• American Petroleum Institute (API) • American Gas Association (AGA) • Gas Processors Association (GPA) • National Propane Gas Association (NPGA)
Government Facilities	Dept. of Homeland Security – Immigration and Customs Enforcement, and Federal protective Service	• American Society of Civil Engineers (ASCE) • American Public Works Association (APWA)
Healthcare and Public Health	Dept. of Health and Human Services	• American Public Health Association (3)
Information Technology	Dept. of Homeland Security – Office of Cyber Security & Communications	• International Committee for Information Technology Standards (3)
National Monuments and Icons	Dept. of the Interior	• National Trust for Historic Preservation
Nuclear Reactors, Materials and Waste	Dept. of Homeland Security – Office of Infrastructure Protection	• American Nuclear Society (3)
Postal and Shipping	Transportation Security Administration	• United States Postal Service (USPS)
Transportation Systems	Department of Transportation	• American Association of State Highway Transportation Officials (AASHTO) • Aerospace Industries Association (AIA) • Air Transport Association (ATA) • American Trucking Association (ATA) • American Public Transportation Association (APTA) • Association of American Railroads (AAR)
Water	US Environmental Protection Agency (USEPA)	• American Water Works Association • Water Environment Federation • National Rural Water Association

CONCLUSIONS AND RECOMMENDATIONS

The objectives of this paper were: (1) to make the case for and to suggest an open-source framework for the development and maintenance of standards and standards-compliant software that can keep pace with the dynamically changing risk assessment methodologies and standards and (2) to identify and evaluate agencies and organizations that could assume the role of standards developer and that could serve as a nationwide repository for the development of open source software tools to support critical infrastructure risk assessment and management.

A framework was presented, by which national standards, compliant with the NIPP risk analysis and management framework, can be developed and approved within the critical infrastructure sectors. The framework calls for an open source code model in support of each of the sectors and compliant with national standards. Under the open source environment, code is designed, developed, shared, tested, and certified by the IT community in cooperation with the engineering community. This process allows for the dynamic development of tools that can keep pace with the rapidly changing industry standards, which must be continually updated to meet changing national needs. A case was made for this open source approach through examples of the application and benefits of open source software within the critical infrastructure sectors and the expressed need to propel disaster management software tools to the next generation.

In recognition of the resources needed to support this effort, an assessment was made as to which national organizations might assume the lead role in these efforts. Based on its history, position, stature, and audience, it is recommended that ASCE consider taking the lead in moving the industry forward through the development of standards and open source software tools to support the goals outlined in the NIPP. In addition to ASCE, a number of other national organizations were identified as possible leaders of sector-specific efforts in support of the overall effort led by ASCE.

It is believed that adoption of an open source framework to the development of software tools in support of critical infrastructure risk assessment and management will greatly improve efficiency and reduce the costs associated with analysis. Furthermore, this alternative will facilitate cooperation among and between agencies and focus the efforts on critical infrastructure risk and resiliency improvements as opposed to software tool endorsement.

REFERENCES

1. "*About ASCE*". (2011). American Society of Civil Engineers. <http://www.asce.org/AboutNASCE/> (Sept 29, 2001).

2. "*API NPRA SVA*". 2007). Security Analysis and Risk Management Association (SARMA). <http://sarmaNwiki.org/index.php?title=API_NPRA_SVA> (Sept 30,2011).

3. "*ASABE Standards Program*". (2011). American Society of Agricultural & Biological Engineers: <http://www.asabe.org/standards.aspx> (Sept 30, 2011).

4. "*ASDSO eNews*". (2011). Association of State Dam Safety Officials. <> (Nov 9, 2011).

5. ASMENITI. (2009). "*All-Hazards Risk and Resilience*". American Society of Mechanical Engineers - Innovative Technologoies Institute. New York, NY

6. AWWA/ASMENITI. (2010). "*Risk and Resilience Management of Water and Wastewater Systems*". American Water Works Assocation / American Society of Mechanical Engineers N Innovative Technologies Institute. Washington, DC.

7. "*Codes and Standards*". (2011). American Society of Civl Engineers. <http://www.asce.org/codesN standards/> (Sept 29, 2011).

8. "*Commercial Facilities Snapshot*". (2008). Department of Homeland Security. <http://www.dhs.gov/xlibrary/assets/nipp_snapshot_commercialfacilities.pdf> (Oct 4, 2011).

9. "*Critical Infrastructure*". (2010). Department of Homeland Security. <http://www.dhs.gov/files/programs/gc_1189168948944.shtm> (Sept 27, 2011).

10. "*Critical Infrastructure Protection*". Department of Homeland Security. <http://www.dhs.gov/files/programs/critical.shtm> (Sept 27, 2011).

11. "*Errata to Guidelines for Analyzing and Managing Security Vulnerabilities of Fixed Chemical Sites*". (2002). American Institute for Chemical Engineers. <http://www.aiche.org/uploadedFiles/CCPS/Publications/Print/GL_for_SVA_Errata.pdf> (Sept 30, 2011).

12. "*FASCAT 3.0 Guidance*". (2011). FoodSHEILD. <https://www.foodshield.org/fascat/docs/v3guidance.pdf> (Sept 29, 2011).

13. "*Guiding Principles for the Nation's Critical Infrastructure*". (2008). American Society of Civl Engineers. <http://www.asce.org/Infrastructure/GuidingNPrinciplesNforNtheNNationNsNCriticalN Infrastructure/> (Sept 29, 2011).

14. "*HAZUS*". (2011). Federal Emergency Management Agency. <http://www.fema.gov/plan/prevent/hazus/> (Sept 27, 2011).

15. Laefer, S. M. (2010). "An OpenNSource Vision for HAZUS". *ASCE Journal of Computing in Civil Engineering*. 24 (1).

16. "*National Infrastructure Protection Plan: Agriculture and Food Sector*". (2008). Department of Homeland Security. <http://www.dhs.gov/xlibrary/assets/nipp_snapshot_agriculture.pdf> (Sept 29, 2011).

17. "*National InfrastructureProtection Plan*". (2009). Department of Homeland Security. Washington, DC.

18. "*New Study to Investigate Use of Open Source Software for Securing the Energy Industry*". (2011). from Oregon State University Open Source Lab. <http://osuosl.org/about/news/pr/energysec> (Sept 27, 2011).

19. "*Open Source Alternative to Deploying Transportation Management Systems*". (2010). Research and Innovative Technology Administration. <http://www.pcb.its.dot.gov/t3/s101020_opensource.asp> (Oct 5, 2011).

20. "*Open Source Initiative*". (2011). Open Source Initiative. <http://opensource.org/> (Sept 27, 2011).

21. Opsahl, A. (2011). "*Open Source Software Helps an Oregon Transportation Department for GIS, Website Development*". Government Technology: Solutions for State and Local Government. <http://www.govtech.com/eNgovernment/OpenNSourceNSoftwareNOregonNTransportation.html> (Sept 27, 2011).

22. "*OSI Certification Mark and Program*". (2007). Open Source Initiative. <http://opensource.linuxN mirror.org/docs/certification_mark.php> (Sept 27, 2011)

23. Perens, B. (1999). "*The Open Source Definition*". Open Sources: Voices from the Open Source Revolution. O'Reilly Media. Sebastopol, CA.

24. "*Risk Self - Assessment Tool for Stadiums and Arenas*". (2009). Department of Homeland Security. <http://www.dhs.gov/files/programs/gc_1259861625248.shtm> (Oct 4, 2011).

25. "*Sandia's CANARY software protects water utilities for terrorist attacks and contaminants, boosts quality*". Sandia National Laboratories. <https://share.sandia.gov/news/resources/news_releases/canary/> (Oct 5, 2011).

26. "*SOCMA's Chemical Site SVA Model & Manual*". (2011). Society of Chemical Manufactures and Affiliates. <http://www.socma.com/productsAndServices/?subSec=5&sub=67&articleID=153> (Sept 30, 2011).

27. Tabor, G., Jarman, D., Andoh, R., Butler, D., Galambos, I., Djordjevic, S. (2011). "Application of Open Source CFD in Urban Water Management". *World Environmental and Water Resources Congress 2011: Bearing-Knowledge for Sustainability,* 1464N1471. Palm Springs, CA.

28. "*TSA Information Collection Request–DHS-VISAT-T*". (2009). Chemical Facility Security News. <http://chemicalNfacilityNsecurityNnews.blogspot.com/2009/02/tsaNinformationNcollectionNrequestN dhs.html> (Oct 4, 2011).

29. "*United Nations' Food & Agriculture Organization Selects MySQL as its Open Source Database Standard*". (2006). LinuxPR. <http://linuxpr.com/releases/8687.html> (Oct 5, 2011).

30. "*Vulnerability Assessments*". (2010). FedCenter. <http://www.fedcenter.gov/assistance/facilitytour/drinking/vulnerability/> (Oct 4, 2011).

31. *Welcome to the Open ISES Project.* The Open ISES Project <http://openises.sourceforge.net/home02.html> (Sept 27, 2011).