CoreSHIELD Strategy

2012-2017

National Center for Food Protection and Defense

Table of Contents

You've got to think about big things while you're doing small things, so that all the small things go in the right direction."

— Alvin Toffler

Introduction

Each day we uncover emerging threats to our global populations. Whether natural or man-made, protecting our populations is non-negotiable. Each day professionals around the globe are committed to ensuring the safety and health of their citizens from providing sufficient calories to responding to natural and intentional catastrophes. A meteorological, terrorist, or economic disaster anywhere has ripple effects in our highly integrated global environment. This poses considerable challenges in protecting our population and critical infrastructure. Additionally, a significant portion of our critical infrastructure is privately owned and operated. Collaboration and information sharing between public and private interests is essential in meeting the globe's challenges to be resilient. The multitude of individuals, agencies, and companies involved in doing global good require a robust Information Sharing Environment (ISE).

To meet these essential communication and collaboration needs a Common Organizational Registry Environment was created in a web-based platform called CoreSHIELD. The platform is a central portal where professionals around the globe work collectively to safeguard our populations through secure, integrated resources that enable capabilities such as document management and sharing, online collaboration and meetings, just-in-time training, and contact look-up. Initially developed to support US Food and Agriculture, CoreSHIELD has evolved into an effective ISE for professional and multi-disciplinary communities to accomplish their work efficiently and effectively. A recently released federal report characterized the Common Organizational Registry Environment utilized by CoreSHIELD as a best practice, stating,

> "...the Food & Agriculture sector has piloted and demonstrated the efficiency of building business processes around a Common Organizational Registry Environment (CORE) that allows thousands to partner and improve sector resilience through adaptive outreach and data fusion...The foundation of CoreSHIELD is the taxonomy of roles (e.g., state vet, regional epidemiologist), commodities (e.g., meat, beans), processing functions (e.g., slaughter, ship, audit), and capabilities (e.g., analysis, production, audit), which enable partner organizations (e.g., governments, labs, private sector companies) to link their employees and databases, and form role-driven collaboration activities. This approach has been widely accepted in the sector and has enabled rapid and holistic response to events."

History/Background

CoreSHIELD was developed and is maintained by the National Center for Food Protection and Defense (NCFPD), a Department of Homeland Security National Center of Excellence at the University of Minnesota. The Center received a $2 million USDA Cooperative State Research Education and Extension Service (CSREES) grant in 2005 to demonstrate the ability to create and support a national web-based system that could act as a primary gateway to communication, collaboration, education and training with and between the stakeholders charged with protecting and defending the food supply. As a result of the CSREES grant, NCFPD created a highly successful portal-based system called FoodSHIELD providing a flexible, user-friendly tool to enable homeland-security-related communication and collaboration on a national level. Today, CoreSHIELD serves as the underlying framework for FoodSHIELD and several additional portals and applications that have been added to the NCFPD portfolio of Information Sharing Environments (ISEs) since 2005. CoreSHIELD provides the web-based platform for these secure portal systems, housing databases of current information regarding regulatory agencies, laboratories, and role-based contacts. CoreSHIELD was designed for scalability, enabling it to expand and integrate additional systems when and as needed.

Due to the success of CoreSHIELD and its portals, other communities have recognized its utility in connecting individuals through a web-based ISE. CoreSHIELD has begun providing support to these communities, including the Chemical Sector and most recently the United Nations Food and Agriculture Organization (FAO). The FAO project has created a private and public capability to link professionals across the globe to engage in One Health discussions.

Vision, Mission, and Value Propositions for Stakeholders

Vision

Be the preferred communication and collaboration platform for communities that are geographically or organizationally separate yet need to communicate, collaborate, educate and train together.

Mission

Enable the secure exchange of information for professionals and communities by unleashing the power of community building and collaboration in a secure environment.

Value Propositions

Governments: CoreSHIELD provides local, state, and country-level government agencies a robust platform that connects the community stakeholders to a centralized online environment in which they can build virtual communities for sharing information, collaborating, and managing emergencies.

Private Sector: CoreSHIELD provides private sector entities that own and operate the majority of this world's infrastructure, an opportunity to integrate themselves into virtual communities where their government and NGO partners communicate and collaborate. CoreSHIELD also provides private sector entities a means of identifying appropriate government resources in the case of an "event."

Non-Governmental Organizations (NGOs): CoreSHIELD allows NGOs who traditionally operate on small budgets a mechanism to work with their community partners. The capabilities in the portal structure offer a virtual collaboration space to coordinate their efforts.

CoreSHIELD Architecture And Characteristics

CoreSHIELD is an ISE that provides shared functionality and databases to a suite of portal applications related to a community (e.g. public safety, food security, critical infrastructure protection), enabling secure collaboration, communication, training, and document sharing among users. CoreSHIELD houses the shared document management system and contact information database used by the various portals. Likewise, CoreSHIELD provides the rapid application development code-base that enables webinars and on-line meetings, workgroup set-up, and personalized portal capabilities used by the portfolio of applications that rely on CoreSHIELD. Housing code and data used in a number of applications within a single shared framework enables CoreSHIELD to leverage functionality, features, and costs among its various constituent applications.

Through the evolution of CoreSHIELD, several unique capabilities have been built to support the platform's varying user groups. Sponsors of CoreSHIELD and its various portals and applications are able to leverage the investments of others, as these capabilities have been made available to all. The following list highlights many of the beneficial characteristics of the platform.

- Robustness: CoreSHIELD has a wide variety of capabilities to meet the challenges of information sharing. The platform has been tested through years of prototyping and direct feedback from end users and has demonstrated its ability to recover gracefully from a range of exception situations. The system has developed tools that facilitate sharing and collaboration through multiple means at the discretion of stakeholders.

- Flexibility: The platform has demonstrated versatility and adaptability to meet stakeholder needs, for example; in 2011 after the Japanese earthquake crisis, the platform quickly supported the FERN network to ensure rapid sharing of lab information based on new requirements for inspection.

- Rapid development: To best serve an organic and changing landscape, CoreSHIELD utilizes rapid application development technologies to meet new and emerging threats as required. This rapid development technology is based on enterprise tested and trusted Java platform Enterprise services.

- Leveragability of core capabilities: Critical to long term sustainability and success is the ability to leverage functionality and features created for a stakeholder in one portal and deploy it to all portals. Collaborative development insures a smarter, more capable system by taking the most robust and innovative ideas from a wide knowledge base of subject matter experts and users. The platform allows any of the portals to share services and applications between each other. This reduces the development and integration costs to partners, and provides a reliable framework for sharing data sets and core functions granularly and securely.

- Open IT infrastructure: Transparency and attention to open source capabilities are a part of the CoreSHIELD systems development planning process. Currently, CoreSHIELD has a variety of open source protocols, file formats and applications securely integrated into the platform. This has reduced costs and improved functionality for our stakeholders and continues to be an important principle.

- System interoperability: CoreSHIELD provides the infrastructure that allows user communication and collaboration. In addition, sector or activity specific organizations can build customized portals on the platform for their unique needs. The customization is best represented in the applications that are available for each sector.

Figure 1 depicts a model of how the various portals and applications created for stakeholder agencies rely on and are supported by the underlying CoreSHIELD technologies. For the sake of simplicity, this model shows only some of the CoreSHIELD portals and applications, but several others exist. By relying on the same platform, all of the CoreSHIELD portals can take advantage of CoreSHIELD functionality such as contact database searches, workgroup creation, webinars, and document management.
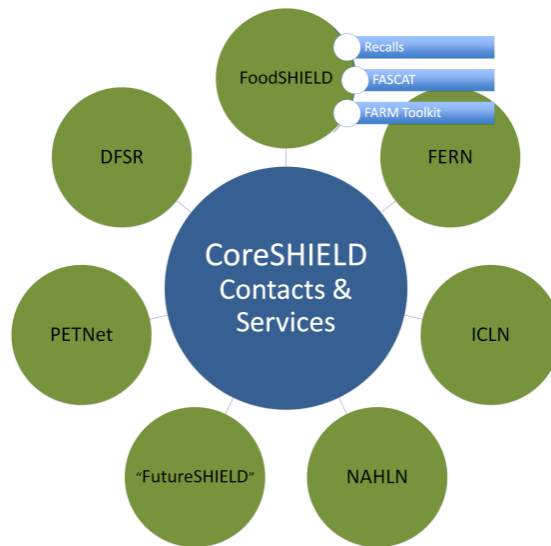

Figure 1. CoreSHIELD Platform - Relationship of Portals and Applications.

Each portal hosts Core applications that provide tools for collaboration that are standard on all portals. These include but are not limited to document management, calendaring, web-meetings, and directories. In addition to the standard, core applications are unique applications that have been built for specific community portals. Traditionally, the applications are relevant only to the community that requested them. Instances where multiple communities have been able to leverage technology are prominent. The laboratory communities are a prime example of this.

Strategic Initiatives

The CoreSHIELD 5-year strategic plan will focus its efforts on strategic initiatives that stabilize the capability as a program now and for the future. NCFPD recognizes that important and essential work is conducted each day on the platform. We understand the criticality of this work and remain dedicated to stabilizing and evolving the platform to meet the ever-changing environment of work and technology.

Strategic Initiative 1: Redesign Stakeholder-Centric Governance Structure and Requirements-Driven Activities

The community using the platform best understands their requirements. NCFPD will regularly and continually gather stakeholder requirements. Each of the requirements will be assessed and validated. The assessment will include utility, technical feasibility, and comparison of other capabilities on the Core that could be leveraged. Sponsors and stakeholders will receive the assessment along with the requirement costs and timeline for development. On occasion, NCFPD may determine the requirement would benefit the entire platform and either fund or attain funding for the request.

CoreSHIELD has benefited from strong stakeholder participation in the existing governance structure. The dedicated and thoughtful participation of stakeholders has allowed CoreSHIELD to better understand user needs and provide new research and development capabilities. As indicated earlier, the initial effort began in 2005 with an USDA/CREES grant. Since this early investment the platform has rapidly expanded through creation of portals and development of applications. Today, 15,757 user accounts and 2,550 working groups have been created in the CoreSHIELD platform. This continued expansion requires us to reassess our current governance model and redesign to meet growing requirements and users.

Three new structures will be established to manage CoreSHIELD. Each of the three will have a unique role to ensure the platform meets the user needs while evolving for future environments.

- **CoreSHIELD Strategic Council** will consist of officials that are currently funding the CoreSHIELD platform, portal(s), or applications. These officials have the direct funding authority and/or decision making for their activities on the platform. The Council provides strategic vision and will jointly ensure the long-term sustainability of CoreSHIELD through appropriate investments. The Council will meet bi-annually. NCFPD leadership will hold two seats on the Council. A charter will be created to document the bylaws of the Council.

- **CoreSHIELD User Advisory Committee** will be comprised of direct users that are members of at least one CoreSHIELD portal. A user from each of the currently funded portals will be required to participate in this Committee hence the size may be adjusted at anytime between meetings. The Committee provides tactical guidance for CoreSHIELD near-term efforts, feedback on platform updates, and critique of current activities. Committee meetings will occur monthly via webinar. A designated member of the NCFPD leadership team and the CoreSHIELD coordinator will hold seats on the Committee. A charter will be created to document the bylaws of the Committee.

-

- **NCFPD Internal CoreSHIELD Governance** will include NCFPD leadership, staff, and the supporting contract vendors. NCFPD leadership is responsible for the review and authorization of new CoreSHIELD related project requests and opportunities to ensure that all activities undertaken meet the CoreSHIELD mission and fall within NCFPD's scope and capabilities. These activities may be generated by user requirements, requests, or developed internally. The NCFPD IT project manager for CoreSHIELD provides the management to ensure project priorities are established and maintained, customer requirements are met, and timelines and budgets are adhered to. To manage platform changes, a Change Control Board has been established. This Board meets at monthly intervals to review, prioritize, author requested changes, new technologies and upgrades. Members of the Board will include NCFPD leadership, NCFPD IT project manager, and CoreSHIELD technical manager (contract vendor). The composition of this Board will undergo review annually.

Strategic Initiative 2: Standardize and Solidify CoreSHIELD Funding

…. FoodSHIELD can be considered a successful experiment and now we need to fund the operations and management...
- Senior U.S. Federal Official, August 2011

Initial funding to support a virtual collaboration capability came in 2005 from an USDA/Cooperative State Research, Education, and Extension Service (CSREES) grant. This grant began the directory components and evolved into the first version of FoodSHIELD. Since this time, a federal agency or stakeholder group has traditionally funded the development of individual portals and applications. While in development, stakeholders have access to a virtual helpdesk that provides users support to all components of the CoreSHIELD platform. The operations and maintenance of the CoreSHIELD platform, portals, and applications have been funded by NCFPD, its vendors, and on some occasions by project sponsors. This cost has included webinars and failover capability.

We recognize that each day essential activities are accomplished on the various components of the CoreSHIELD platform. These include efforts such as, collaborating lab activities during a foodborne outbreak, assessing what is critical in our infrastructure that must be protected, and linking professionals globally to improve the health for humans, animals, plants, and the environment. The CoreSHIELD platform supports day-to-day work as well crises response and management. This platform is proven and must transition to sustainable, programmed funding to ensure stakeholders have the tools they need to meet their responsibilities. This transition requirement is a testament to developers and stakeholders who created a successful capability that now needs to be evolved to a formal program. In this initial strategy year, three cost models will be developed and presented to sponsors.

Cost Model 1: Whole of Government.

All levels of government have acknowledged the benefits of the CoreSHIELD and component capabilities. From the local county to senior leaders within federal departments, users continue to do their work on the platform whether it is managing documentation, sharing lab results, or conducting virtual meetings to eliminate in-person meeting costs. This includes usage by government agencies and organizations that do not or have never funded any component of CoreSHIELD. Due to the innovative development of CoreSHIELD, the government sponsors have been able to continually leverage each other's work. This philosophy has ensured significant cost savings for new capabilities and communities to work on CoreSHIELD components.

To leverage previous efforts and maximize federal usage, NCFPD has developed a Whole of Government cost model. This model would allow any government employee (local, state, and federal) to operate on the portal. While this cost model deviates from current funding models, it shows a strong advantage in allowing all of government to utilize capabilities without individually having to find operations and management funds, which may be significantly troublesome for some organizations particularly at local and state levels. Additionally this consistent and programmed funding would allow us to dedicate teams to development, operations, and maintenance of CoreSHIELD and all its components.

In this cost model, a single operations and maintenance fee would be identified for funding agencies to cover individually or collaboratively. Development work for new capabilities would be funded by the sponsoring organization requesting the development.

Cost Model 2: Sponsor-Driven Cost Model

The components of CoreSHIELD (portals and applications) have been historically funded in two different ways. The simplest funding is direct funding from a sponsor in support of a portal or application they lead. In a few occasions, multiple agencies or organizations are responsible for a portal. For example, FoodSHIELD has been funded by multiple federal agencies to support the various stakeholders across agencies with responsibilities for food and agriculture.

The Sponsor-Driven Cost Model will build tiers for each CoreSHIELD component. Costs for development and operations/maintenance on the platform will be divided into two categories: Operations Maintenance Fee and New development. Pre-established tiers based on size and usage of the component will charge portals and applications.

Cost Model 3: Metric-Driven Cost Model

This cost model will be developed and priced based on platform usage. Metrics, for pricing, will be pre-identified and continually tracked to capture the activity occurring on each portal or application. Sponsoring agencies will be charged an operations and maintenance fee based on the annual assessment of metrics. Portals and applications with multiple sponsors will be charged equal portions of the fee. New development will be charged separately based on sponsor requirements.

Strategic Initiative 3: Security, Standardization and Documentation

Changes in Information Technology (IT) remain constant with continuous evolutions to the environment each day. This rapid development and product entry into the commercial market has created challenges to implementation of technology standards that stay ahead of deployment. NCFPD has and will maintain awareness of the security landscape and bring forth various emerging technologies to combat the ever-changing threat vectors and face-off hacking attacks. We evaluate and test various approaches to provide comprehensive security coverage, and to accomplish this requires consistent testing. Defense-in-depth and Unified Threat Management are basic principles. We recognize we must remain vigilant to documentation, security assessments, and industry standards to meet the evolution and threats of the IT environment.

Currently, CoreSHIELD follows the National Institute of Standards and Technology (NIST)/Federal Information Security Management Act (FISMA) security framework to ensure adherence to all federal regulations. The platform meets the moderate baseline requirements. Using high security controls for all users, we ensure that files and data are fully encrypted while at rest in addition to in transit. The security team will continue to monitor emerging requirements from NIST, including new FISMA guidance for cloud based systems, as well as recently adopted principles for EMAP (Event Management Automation Protocols). We will track agency-specific direction to determine impacts in security measures that apply to CoreSHIELD.

This strategic initiative will begin with a thorough assessment of current technology. The assessment already underway, focuses on a) documentation of all IT architecture; b) technological architecture audit; and c) an external security audit of CoreSHIELD, portals, and applications. Once the assessments have been completed, a list of gaps will be developed and prioritized, with recommendations for addressing the gaps. NCFPD leadership and technical advisors will determine the timeline for implementation of the recommendations. Each year external technology and security assessment will be accomplished. Annual results will be incorporated into a prioritized list of recommendations for implementation.

Within 24 months, CoreSHIELD will examine the National Information Exchange Model (NIEM) standards to determine desirability of working towards establishing NIEM compliance. This exchange framework represents a partnership of government organizations and the private sector dedicated to effectively sharing critical information for public safety and homeland security.

Strategic Initiative 4: Expand Educational support for CoreSHIELD Users and Administrators

A critical asset to a large infrastructure is education. Creating an engaging training and education program for users of CoreSHIELD portals and applications is an ongoing and growing effort. To be effective with users that are overwhelmed with daily duties, innovative and exciting training approaches will be planned to shepherd users from a general knowledge level to power users and specialists in the system. Initial education efforts will focus on exploring the learning needs of the full range of current users. Assessments are currently underway to understand the competency of users across all

CoreSHIELD portals. This information will allow for targeted education and training to ensure users are benefiting from what the platform has to offer.

Within one year of this strategy, NCFPD will release a training program comprised of curriculum designed to meet beginner through advanced user needs. The program offerings will be cataloged with each entry articulated by a thorough description and course objectives. Where course gaps exist, as identified by the training assessments, new courses will be designed and constructed. These courses will be tested for effectiveness and strategically added to the CoreSHIELD training catalog. Where appropriate we will initiate required activities to obtain continuing education granting privilege for Continuing Education Units (CEUs).

CoreSHIELD education and training staff will work to establish formal procedures to route requests and questions from users before, during, and after training to the right person within the NCPFD. We believe that fulfilling these requests advances their user knowledge base and competency on the platform thus maximizes the benefits they obtain by using it.

Strategic Initiative 5: Expand and Refine Community Engagement Activities.

CoreSHIELD is the result of food and agriculture professionals coming together to find an improved way to communicate with each other. The creation of their first virtual sector directory planted the seed for the platform that we have today allowing food and agriculture professionals to efficiently accomplish their work without limitations of information or geographic separation. Based on the success of CoreSHIELD portals, other sectors and organizations have developed an interest in the platform and what it can do for their community. Recognizing that both current and potential stakeholders have requests, CoreSHIELD outreach activities will have a bifurcated approach to community engagement.

Membership outreach is a critical piece to the CoreSHIELD plan. In 2012, NCFPD will conduct a stakeholder survey to understand their usage, requirements, and communication desires. This information will lay the foundation for a robust engagement plan that will lay out the engagement strategy over the course of the next five years. From previous dialogue with our members we know that the engagement plan will include the following in addition to what we learn from the survey.

- Development of a consistent, multi-delivered communications.
- Formal process for routing user requests to the right person in the NCFPD to include escalation for complex issues
- Incorporating social media
- Actively supporting member on-boarding and startup activities.

We commend the food and agriculture sector for not only championing an ISE but for driving new, innovative ways for the platforms to be used so stakeholders could meet their mission. This hard work has led to interests from other sectors and organizations to build capability for their communities. The initial step is the creation of a platform development engagement plan. NCFPD will use this plan to discuss the capabilities and new organization requirements of an ISE. This plan will be used for both those organizations requesting information on the platform as well as marketing to organizations that

may benefit from the platform. Adding new communities to the platform benefits all stakeholders through technology development and cost sharing of CoreSHIELD capabilities.

Strategic Initiative 6: Deliver Cutting Edge Technology

We live in a magnificent and impressive time for IT. New developments to the IT marketplace are swift and unapologetic. The impact of cutting edge technology can be remarkable however the incorporation of consistent evolutions in the field may be overwhelming. With the race to get technology to commercialization we, as a society, have learned that not all technology is useful. We owe it to our members to remain on the cutting edge of technology; however we pride ourselves in providing good analysis of new capabilities and wise incorporation of IT that benefits the incredible work that happens on the CoreSHIELD platform each and every day.

Over the course of this strategy, we will take a multidirectional approach to identifying and implementing new technology. IT will be reviewed and analyzed in one of two categories, immediate and visionary. Each of the two categories will have criteria for assessment. The immediate category will be defined as cutting edge technology that is currently available and could be implemented into any component of the CoreSHIELD platform. The visionary category will represent cutting edge technology that is in development, beta testing, or newly released and would be implemented into CoreSHIELD no sooner than 12 months from the time of identification.

Several technologies that currently exist have been identified as having potential benefit to CoreSHIELD users. These technologies will be assessed and if appropriate incorporated into the suitable CoreSHIELD components.

Immediate Category

- Push notifications and alerts driven by user-preference (text and audio)
- Instant messaging and Live Chat
- Geographic Information System (GIS)
- Social media

Visionary Category

- New application programming interfaces
- Mobile platforms

Conclusion

Each day NCFPD hears success stories of how CoreSHIELD portals and applications have made a difference in accomplishing agency work or networking communities together in new and unique ways. To ensure this ISE continues we must transition to a formal and structured program with dedicated teams that support the various stakeholders across our users' communities.

The six strategic initiatives offer a roadmap to make CoreSHIELD sustainable for the future. Each initiative is distinctly written, but on its own does not accomplish the vision for the platform. As we look back in 2017, this strategy will be considered a success because NCFPD, sponsors, and users accomplished the work as a team. NCFPD looks forward to the journey.