19th ICCRTS
"C2 Agility: Lessons Learned From Research and Operations"

For the paper titled:

Achieving Information Dominance: Unleashing the Ozone Widget Framework

Topic Area

Topic Area 3: Data, Information, and Knowledge

Alternate Topic Areas

Topic 2: Organizational Approaches, Collaboration, Social Media/Networking

Topic 1: Concepts, Theory, and Policy

Colonel Kathy Conley (U.S. Air Force – Retired)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311

Captain George Galdorisi (U.S. Navy – Retired) - POC
Mr. Brent Brockman
Ms. Patty Diercks
Ms. Amanda George
Ms. Wanda Lam
Ms. Analiza Lozano
Ms. Rita Painter
Mr. Glenn Tolentino

Space and Naval Warfare Systems Center Pacific
53560 Hull Street
San Diego, California 92152-5001
(619) 553-2104
george.galdorisi@navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Achieving Information Dominance: Unleashing the Ozone Widget Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 16-19 June, 2014 in Alexandria, VA.

14. ABSTRACT

One of the key lessons learned from analysis of Joint operations is the information that was available to operations planners was not discovered and therefore not utilized ? impeding the flow from data, to information, to knowledge, and typically leading to suboptimal results. This challenge is exacerbated when information could ? and should ? be drawn from multiple enclaves from NIPRNET, to SIPRNET, to JWICS. Sharing this information DoD- and agency-wide has been an ongoing challenge. We will share details of emerging research currently underway in a collaboration between the Naval Postgraduate School and the Space and Naval Warfare Systems Center, Pacific to make essential information residing in multiple classification enclaves discoverable, accessible, widely shared, and understandable by those who need the information. The current approach utilizes SWIF (Secure Web Integration Framework) and employs OWF ? utilizing widgets for data input and retrieval ? to make products viewable and retrievable by the DoD community, and ultimately the interagency community, both on the high and low side. The design approach creates an accredited software program for NIPRNET, to SIPRNET, to JWICS and a web-based approach that enables users to access multiple databases. This approach is being beta-tested at the Naval Postgraduate School and involves a process to make classified student theses and other Naval Postgraduate School research products available to a wide-range of users who previously did not have access to these products. Once this small beta-test is complete, Space and Naval Warfare Systems Center, Pacific engineers will expand the use case to the Office of the Secretary of Defense and the Joint Staff, ultimately making tailored information more discoverable, accessible, widely shared, and understandable by the end-users.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**58**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Abstract for
Achieving Information Dominance:
Unleashing the Ozone Widget Framework

One of the key lessons learned from analysis of Joint operations is the information that was available to operations planners was not discovered and therefore not utilized – impeding the flow from data, to information, to knowledge, and typically leading to suboptimal results. This challenge is exacerbated when information could – and should – be drawn from multiple enclaves from NIPRNET, to SIPRNET, to JWICS. Sharing this information DoD- and agency-wide has been an ongoing challenge.

We will share details of emerging research currently underway in a collaboration between the Naval Postgraduate School and the Space and Naval Warfare Systems Center, Pacific to make essential information residing in multiple classification enclaves discoverable, accessible, widely shared, and understandable by those who need the information.

The current approach utilizes SWIF (Secure Web Integration Framework) and employs OWF – utilizing widgets for data input and retrieval – to make products viewable and retrievable by the DoD community, and ultimately the interagency community, both on the high and low side. The design approach creates an accredited software program for NIPRNET, to SIPRNET, to JWICS and a web-based approach that enables users to access multiple databases.

This approach is being beta-tested at the Naval Postgraduate School and involves a process to make classified student theses and other Naval Postgraduate School research products available to a wide-range of users who previously did not have access to these products. Once this small beta-test is complete, Space and Naval Warfare Systems Center, Pacific engineers will expand the use case to the Office of the Secretary of Defense and the Joint Staff, ultimately making tailored information more discoverable, accessible, widely shared, and understandable by the end-users.

Paper for
Achieving Information Dominance:
Unleashing the Ozone Widget Framework

Background

"The continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control."

- U.S. Joint Chiefs of Staff's Joint Vision 2020

As the *Joint Vision for 2020* points out, the importance of getting the right information to the right individuals in the conduct of military operations cannot be overstated. Indeed, the importance of information in the realm of command and control of military operations has increased as data inputs have expanded exponentially in the information age. As the *Joint Vision* states, "advances in information capabilities are proceeding so rapidly that there is a risk of outstripping our ability to capture ideas, formulate operational concepts, and develop the capacity to assess results."[1] Given the necessity of having access to the right information, at the right time, the U.S. Department of Defense (DoD) and the U.S. Navy have focused heavily on ensuring that the warfighter is able to dominate the information sphere.

The operating environment described in the recently released *Quadrennial Defense Review* (QDR) has been "is increasingly enabled by technology, which provides the types of capabilities once largely limited to major powers to a broad range of actors." [2] These technologies have enabled even individual actors to achieve a large set of pertinent information for use against our warfighters. Given the increased competition, and indeed threats, in the information environment, it has become even more important our information can gathered appropriately from all sources, all classifications, and combined into a cohesive and useful data set. Providing a framework to sift, organize, and agilely share information received is vital if everyone in the military organization is to achieve the ability to make efficient and timely decisions. As the U.S. Joint Chiefs of Staff state, "decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary."[3]

[1] United States Chairman of the Joint Chiefs of Staff. *Joint Vision 2020.* Department of Defense. 2012. Pg. 8.
[2] Department of Defense. *Quadrennial Defense Review 2014.* Department of Defense. 2014. Pg. 3.
[3] United States Chairman of the Joint Chiefs of Staff. *Joint Vision 2020.* Department of Defense. 2012. Pg. 8.

The sheer volume of information flowing from different parts of the military structure has created unique problems. One information challenge, in particular, that has continued to plague military command and control and military planning is the need to move information effectively and smoothly between different security domains. Military planners in particular need to both receive all the information, no matter the security classification, but also to pass the information relevant to the plans of action to their action officers who may have different security classifications. Too frequently is information "siloed" by it classification system, with necessary data residing on one or all of these networks: unclassified Nonsecure Internet Protocol Router Network (NIPR), classified Secret Internet Protocol Router Network (SIPR), or TOPSECRET Joint Worldwide Intelligence Communications System (JWICS). While this challenge is rampant within a single service, it becomes even more difficult when the planned mission needs to incorporate more than one service or more than one nation. As the QDR states, "the Department of Defense remains committed to working with industry and international partners as well, sharing threat information and capabilities to protect and defend U.S. critical infrastructure, including in our role as the sector-specific agency for the defense industrial base."[4] Thus, the DoD is facing a challenge in which the different classification levels within services, between services, and between allies, are causing information to not get to the right people at the right time.

As the *U.S. Navy's Information Dominance Roadmap* emphasizes, the U.S. Navy is grappling with the problem of ensuring it can "maintain essential network and data link services across secured segments of the electromagnetic spectrum in order to transport, share, store, protect and disseminate critical combat information." [5] The *U.S. Navy's Information Dominance Roadmap* states the importance of having a system that can reach across secured segments of U.S. Navy's networks; there is currently not a fielded system to address the problem. The U.S. Navy faces a number of unique challenges in passing information out to its deployed fleet, and back to headquarters commands. The limited bandwidth and the need for security while deployed have both contributed to the urgency the U.S. Navy feels to solve this problem. While work on this problem is progressing in other areas, the U.S. Navy's Space and Naval Warfare Systems Center Pacific (SSC Pacific) has brought its experience with command and control as well as programing and networks, to bear on the problem.

Secure Web Integration Framework (SWIF)

SSC Pacific has grappled with the problem of moving information through different security domains in an innovative and agile framework. The use of SSC Pacific's open source and in-

[4] Department of Defense. *Quadrennial Defense Review 2014.* Department of Defense. 2014. Pg. 15.
[5] United States Chairman of the Joint Chiefs of Staff. *Joint Vision 2020.* Department of Defense. 2012. Pg. ii.

house technologies such as OZONE Widget Framework (OWF), the secure web integration framework (SWIF) Security Services, and the Data-Driven Documents JavaScript (D3JS) library, can provide a secure environment where mission planners and analysts can develop comprehensive target systems for effects-based planning. This tool will allow users to build comprehensive political, economic, and social graphical models in direct support of warfighter needs. Information normally residing in multiple classification enclaves, such as NIPRNET, SIPRNET, JWICS, and higher will be accessible and discoverable by mission planners and analysts with a need to know via these interactive graphical models. The web-based interactive analytic planning tool will allow planners to visualize adversary factors such as threat, economic support, and weapons production, in terms of graphical features such as color, shape, and thickness. Drilling down on graphical elements, planners with the appropriate security accesses will have access to detailed target information.

Current analytical tools do not have the security features to handle – and where necessary - harmonize information from disparate classified networks. As a result, planners and warfighters are typically relegated to using static Power Point slides on the high side – resulting in sub-optimal planning and execution. Consequently, key adversary information remains undiscovered and the planner is typically unable to explore alternative scenarios and courses of action. This often results in suboptimal mission planning and in a worst-case scenario, can result in mission failure. The SWIF Security Services provide an interactive analytic tool that allows joint operational planners to visualize and access critical adversary data from multi-domain spaces to produce effective, safe, and successful mission plans. Planners and intelligence analysts will use this tool to develop dynamic models that will answer the "What if"-type questions typically posed by senior leadership and will ultimately enable these leaders to make better decisions, faster, with fewer people and fewer mistakes.

The analytical planning tool will allow planners to dynamically manipulate analytical data on the high side. These planners will be able to collaborate with in-house analysts, analysts from other organizations and subject matter experts from academia and other agencies to discover information on the target system without fear of compromising security or mission success. Planners will have more effective tools that are able to seamlessly leverage all-source intelligence. Hence, they will be better equipped to deliver timely, mission specific plans to the warfighter.

SWIF Mission

SWIF is a web-based framework that allows users to collaborate and share information in a secure environment. SWIF provides different layouts for lightweight applications, called widgets, via a web browser. Information residing in SWIF is available to users who are cleared

for access, yet, restricted to those who are not. The Joint Staff Senior Leadership has endorsed SWIF as a potential solution to address the challenge faced by the Joint operational planning community: Information that was available to planners was not discovered and therefore not utilized – impeding the flow from data, to information, to knowledge, and typically leading to suboptimal results.

SWIF Architecture

SWIF was developed on top of the OWF. Out of the box, OWF provided the capability to quickly deploy lightweight applications. OWF provides a platform for the rapid development and deployment of web-based applications that have the ability to communicate with each other. OWF is a web-based application framework developed by the National Security Agency (NSA) for use in a secure environment. NSA has provided the framework to the open-source community to foster further development and integration. Developed as a secure framework, OWF implements Discretionary Access Control (DAC) at the widget-level. This allows users and groups of users to access specific widgets they are authorized for depending on their role and responsibility. This provides some multi-level security but does not specifically implement security for access to the underlying data that will be utilized by the widgets.

The SWIF development team created several components to add the Mandatory Access Control (MAC) capability to OWF. MAC, the strictest of all levels of control, controls access to the data that differs for all resource objects on the system. Thus, under MAC, each unit of data is assigned a different security level allowing access to be controlled based on the data. The addition of MAC on the data itself in a multi-level security framework, this will provide the security to allow for its use in a variety of multi-institutional settings. The SWIF development team also created an Application Programming Interface (API) to allow any developer to create widgets that are 'MAC enabled.' The extension of the OWF's capability to enable security MAC enhances the sharing and coordination of multi-institutional activities and artifacts within different accesses and classifications.

SWIF Security Model

SWIF implements data access restriction by enforcing MAC on all of its data operations. A user can only access the data which he or she is cleared to view. MAC is implemented at multiple security levels and can be configured based on the security policy of the network on which the framework is deployed. SWIF also implements DAC inherited from OWF to manage permission of widgets based on a user's roles. For example, a user with the Planner role will be granted access to the Plan Editor widget, the Capability Service Provider role to the Concept of

Execution widget; this same user would not be granted access to widgets that were restricted to other roles.

In order to use this construct, all data must be assigned security labels, either from its original source or by users' input. The system will verify the data labels against the user's security accesses upon retrieval and saving of data. This will ensure a user cannot view (read) or label (write) data that are classified above his or her clearance level. This security implementation of MAC at the row (or record) level supports an environment where multi-level data access is required.

SWIF provides a core set of secure web services via a set of ReST API. Developers who want to develop SWIF widgets should use the SWIF JavaScript Services to allow their widget(s) to communicate with the database and other widgets and display appropriate security banners for its content.

SWIF Dynamic Search

SWIF provides a dynamic search functionality that filters results based on user's security accesses. Users can perform searches based on attributes such as keywords, characteristics of the data, security labels, or clearance level, etc., depending on the type of data.

In a prototype developed for the experienced planners in FY13, SWIF widgets with specific search requirements were implemented to aid the planners and intelligence analysts in target and capability selection. Depending on the type of information needed, users could dynamically pull information such as targets, capabilities, courses of action from a plan from the SWIF database based on their roles (via DAC) and clearance level (via MAC). The SWIF Search widgets allowed the planners to select target/capability matches based on fields such as expected effect and target type to incorporate into their plan. Results would only include those capabilities to which the planner had access thereby maintaining MAC.

The search algorithm used in the SWIF Search Capability Widget was a text-based search that could match on multiple fields of the target and capability. Future plans to enhance the Capability Search function will be addressed in the Double-Blind Matching Algorithm section. The prototype effort has demonstrated the viability of SWIF in the Joint planning community.

SWIF is also being considered by the Naval Post Graduate (NPS) School to test a process to make classified student theses available and discoverable to a wider audience. Thesis documents are classified at the file level, preventing individuals without sufficient clearance to obtain relevant information. In most cases, only parts of the document are classified. With the SWIF

dynamic search model, contents will be stored at the record level (as in paragraphs), therefore, are more searchable and available to a wide-range of users who previously did not have access to these products.

Widget developers utilize the SWIF built-in search services via the SWIF ReST API in two forms: searching and querying. The Search API provides the ability to request exact matches explicitly for one or more fields within the collection. The Query API accepts a string of terms and returns results that match one or more terms, along with a score for each result, based on the total sum of occurrences of all terms in all indexed fields.

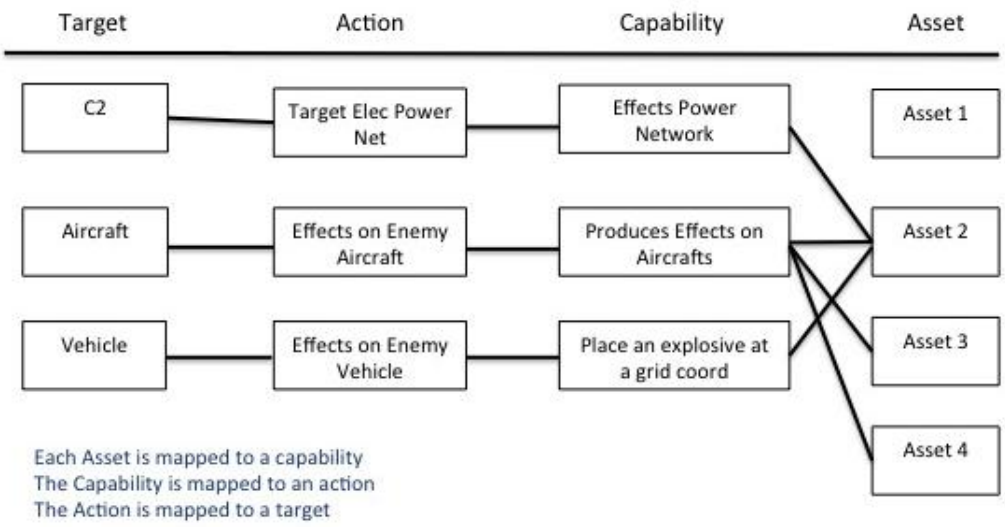
Double-Blind Matching Algorithm

The Double-Blind Matching algorithm was first introduced in the Requirements Capabilities Matching System (RCMS) in a Master's thesis written by Captain Michael Gerson, USMC, at the Naval Post Graduate (NPS) School. RCMS was developed to test the compatibility of Combatant Commands (COCOMs) requirement to the capabilities by a capability provider. The algorithm was designed to match requirements to capabilities, test the match for basic requirements, and optimize match when multiple solutions exist.

Matching results will improve military planning and operations by:

- Validating the matches with information currently not considered or known by the planners
- Meeting basic requirements before effort is expended
- Allowing COCOMs to receive instant response if non-supported
- Reducing the number of irrelevant requests to service providers

Figure 1: RCMS



When integrating within SWIF the Double-Blind Matching technique can be furthered enhanced by MAC to ensure only the users with appropriate security access can see the data. Information regarding the capability program can be stored at multiple security levels to ease the Service provider's concern on need-to-know and who should see what. Planners often run into the issues of not being able to find all the potential capabilities to achieve a desired effect for their plan due to the limited information released by the capability providers.

The enhanced search functionality that employs the Double-Blind matching algorithm can be implemented and added to the framework as part of the SWIF services. Depending on the data, widget developers who utilize this service will be able to define the weight and attributes for matching algorithm.

SWIF Widgets

SWIF widget core capabilities act in concert to support all aspects of mission planning from target selection to concept of operations development. Target widgets focus on providing planners and analysts the ability to diagram and analyze government, economic, and social entities' relationships in support of target and capability selection. Planning widgets allow the user to develop multiple courses of action (COAs) and visualize events within the context of the overall plan. Most importantly, third parties are allowed to use SWIF as a framework for developing, as well as hosting, widgets to enrich core capabilities. Existing non-SWIF widgets

can be rapidly adapted to integrate into SWIF. However, all widgets within SWIF must undergo the SWIF Governance Process for certification and accreditation (C&A) prior to deployment.

SWIF Widget Governance Process

The SWIF goal is to foster innovation rapidly to field relevant capabilities in order to meet existing and emerging collaborative needs amongst all branches of the military and from disparate security access levels. Currently, new capabilities are subjected to lengthy testing and C&A processes. This necessary but lengthy process may take as long as nine months to complete in which time crisis planning needs may be unmet. The SWIF architecture allows for a decoupling of the hosting web-based infrastructure and the widgets where functionality resides. The infrastructure consisting of OWF, SWIF Security Services, and the SWIF database would be subject to the full gamut of C&A review. However, once the infrastructure was certified and accredited, it will only undergo C&A for upgrades - not when new widgets are added. Widgets, on the other hand, would undergo a governance process that would streamline the C&A process based on their capabilities, complexity, and security boundaries.

Widgets are characterized as simple or medium based on their capabilities, complexity and security risk posture in relation to the networks in which they operate and the applications with which they interface. Table 1 delineates the difference between a simple and medium widget category type in SWIF:

Table 1: SWIF Widget Category

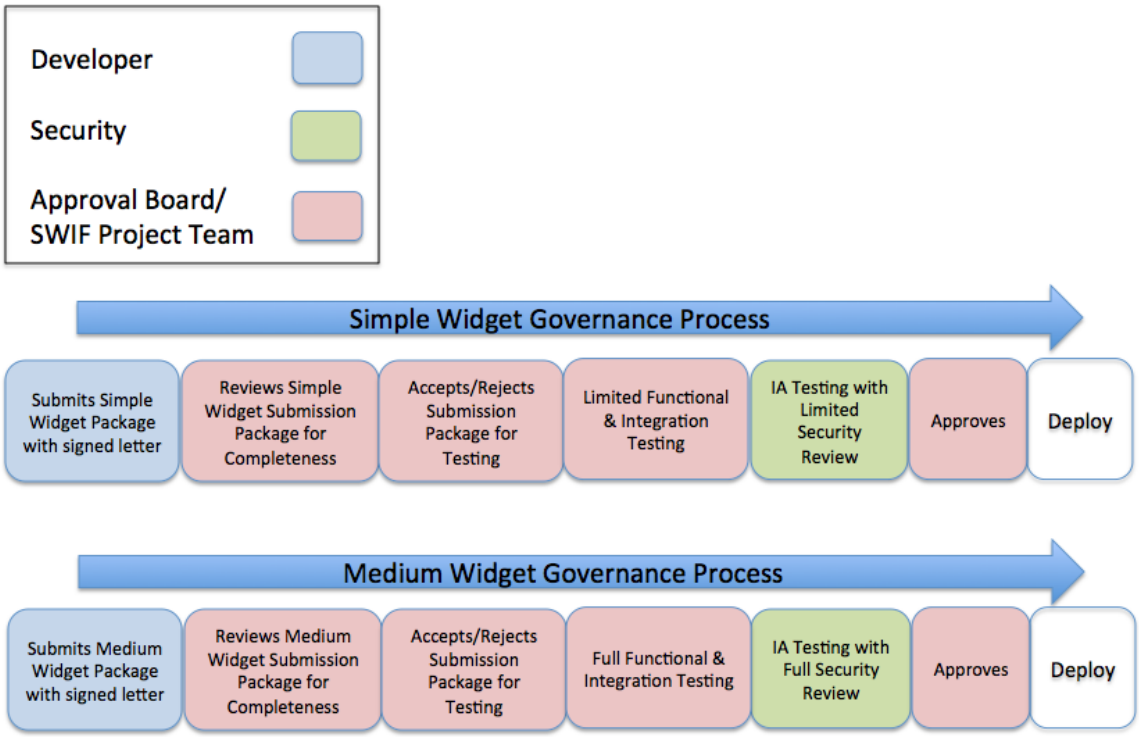
Widget Type	Renders Data from the SWIF Database	Saves Data to the SWIF Database	Inter-widget Communication
Simple	Yes	Yes	No
Medium	Yes	Yes	Yes

Widget approval is dependent upon the residual risks the widget poses to the network in which it operates and the systems it supports. These residual risks are then weighed against mission efficiencies, accuracies and overall improvements the widget creates in specific mission execution.

The widget governance process is streamlined into workflows dependent upon the widget's profile. The Widget Submission Package of medium widgets will undergo a workflow with more rigorous testing and review as compared to the governance workflow for simple widgets. Both the Simple and Medium Widget Governance Workflows can be seen in Figure 2 with color-coded roles. The Developer role (in blue) is responsible for ensuring the Widget Submission Package is complete and submitted appropriately according to the Widget

Submission Package Checklist. The SWIF Project Team/Approval Board role (in light red) is responsible for: reviewing the Widget Submission Package for completeness, functional testing, integration testing, and final approval. Finally, the Security role (in light green) confirms that all Information Assurance (IA) testing is performed appropriately for the widget type. This governance process ensures that widgets are tested properly but without the unnecessary waste of time and effort.

Figure 2: Widget Governance Process Workflow



SWIF Components

There are a variety of components that make up the SWIF construct. These components include an unstructured database, secure web services, API, and banner service.

NoSQL Database

For data storage, SWIF uses a NoSQL database. The main feature of the NoSQL database that SWIF utilizes is the capability to provide a dynamic schema. Standard relational databases have to define all field information ahead of time before you can enter data into the table. Having a

dynamic schema allows the operator to insert data into a collection (table in relational database terms) with different fields for the same collection. In other words, you create a collection to put data into, but you do not define any fields of the collection. This allows a widget to be installed without having to initialize a database to define tables. The simplification of a widget installation enhances the accreditation process because the core system does not have to be changed to install a widget.

SWIF Secure Web Services

Based on the REpresentational State Transfer architectural style (ReST), the SWIF secure web (ReST) services are provided to give access to MAC data stored in the SWIF NoSQL database. The services include standard methods that allow a developer to retrieve, save, update, delete, search, and label a particular data entity. Widget developers are also allowed to insert any fields into a collection as needed. The only requirement with MAC data in the NoSQL database is that every entity inserted into a collection has a security label with the required system security attributes and the user must have the required security accesses to the label. ReST services are url-based and are problematic for widgets when urls are modified. To address this, a JavaScript library was incorporated into SWIF to handle the communication with the secure web services.

SWIF JavaScript API

The SWIF JavaScript API allows the widget to communicate with the SWIF secure web services by executing JavaScript methods from within the widget. This greatly simplifies the process of creating a secure widget by abstracting the complexity of knowing which URLs to call from a widget. See Table 2 for Common SWIF API Methods.

Table 2: Common SWIF API Methods

Method	Parameters	Description
labelCollection	<collectionName> <collection> - JSON collection to label	Display the labeling dialog to set the new label for the collection.
getCollection	<collectionName> <collectionID> or array of collectionIDs	Retrieves data element(s) from the collection.
createCollection	<collectionName> <collectionJSON>	Insert data element into a collection.
updateCollection	<collectionName> <collectionJSON>	Updates a particular data element with new JSON.
deleteCollection	<collectionName> <collectionID>	Deletes a particular data element.
searchCollection	<collectionName> <searchString>	Searches a collection with a given search criteria.

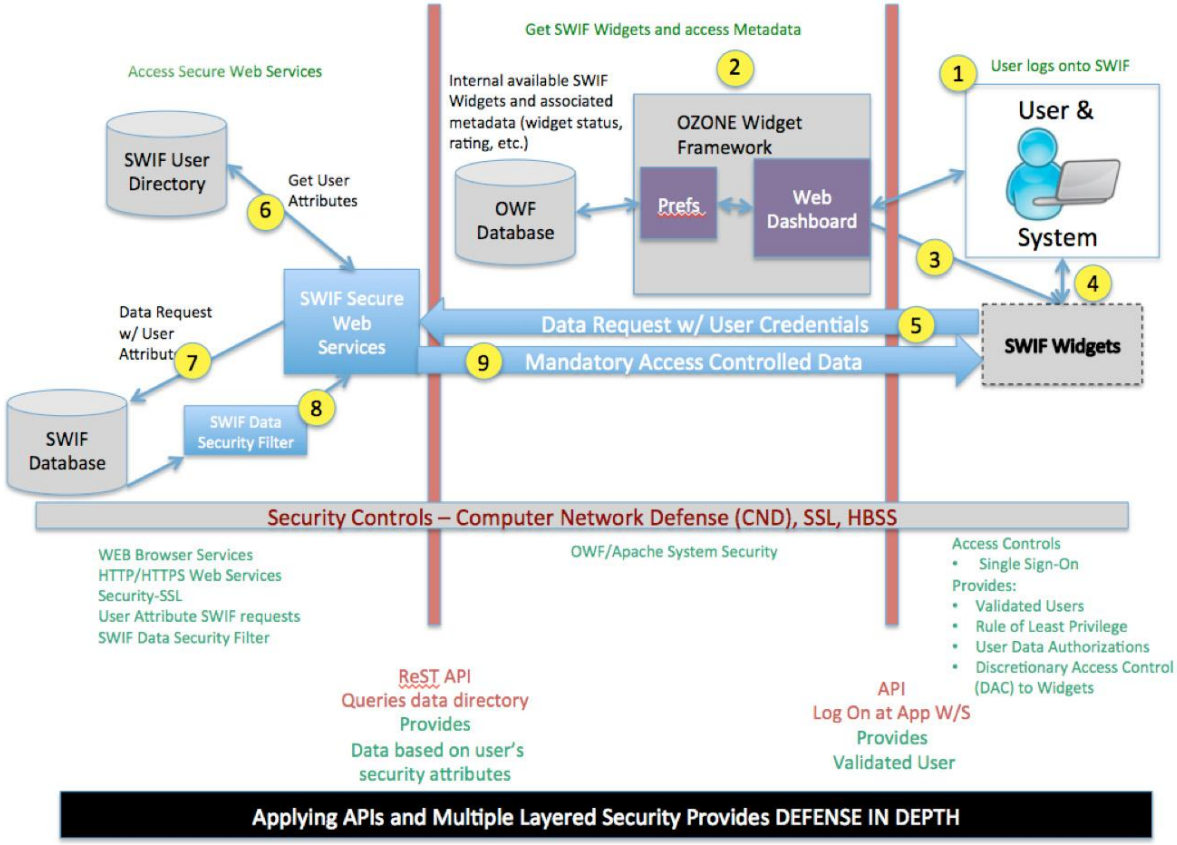
Banner service

SWIF contains a banner service that displays the current security information for all data inside a particular widget. The banner is updated by the JavaScript library whenever data is changed in the widget. This keeps the user knowledgeable of the security of a data residing in a widget. The SWIF banner service also creates a banner at the top of the browser window that is a union of all security labels for all widgets on the dashboard. All banners are always in sync with the data that is contained under them.

SWIF Widget Lifecycle

The SWIF widget lifecycle describes how all of the SWIF components work together. Figure 3 shows the process of the SWIF Widget Lifecycle.

Figure 3: SWIF Widget Lifecycle



1. User logs onto OWF via a web browser.
2. OWF retrieves the users preferences and displays the user's OWF Dashboard that contains the widgets the user has selected to view.
3. User-selected, MAC-enabled, SWIF widgets are loaded onto the dashboard.
4. User interacts with the SWIF widgets that make calls to the secure database.
5. Data requests from SWIF widgets use the Central Authentication Service (CAS) Single Sign-on to pass along the user's credentials with each request.
6. SWIF Services receive all security attributes from the user account.
7. SWIF Services queries the secure database with the user's security attributes. Since the queries contain restraints using the user attributes, no data is returned from the database that the user should not see.
8. For additional security, SWIF services processes the data to ensure user's security attributes match data's security attributes.
9. Requested MAC data returned to the SWIF widget.

Exercise and Usability Testing

After the development of the SWIF prototype January 2013, a three-day event was held at SPAWAR Systems Center Pacific, San Diego, CA to explore (with the planning community) the usefulness of SWIF to accomplish their planning mission. It allowed the demonstration of SWIF as a proof of concept enabling users to actively use the prototype as part of their planning process. The event focused on capturing user community input on SWIF features as well as its operational impact.

The participants included the following:

- Policy support
    - J3 Deputy Directorate of Global Operations (DDGO) Program Support Division (PSD)
- Experienced planning team
    - USSOCOM, USEUCOM, USSTRATCOM, USCENTCOM, USPACOM, JWAC, USAF
- Inexperienced planning team
    - NPS
- Observers
    - Program Office, SSC PAC, NPS, JHU APL

The productive three days provided SSC Pacific with a set of improvements to SWIF. Stakeholders identified attributes that will help SWIF evolve to a refined planning system:

- Ability to identify or search for capabilities to achieve desired effects outside of the current system
- Ability to pull planning and intelligence data from other domains that can easily be manipulated and presented
- Ability to pull all related planning data from a cloud source to the current system
- Improve capabilities by allowing SWIF types of applications with inherited MAC and DAC into a cloud-based secure mail application, similar to Google, Amazon, and Yahoo
- Customer off the shelf products that users would like to see integrated with SWIF to include Google earth, Google Docs, Tablets, and Gmail

The three day event provided a means for users to align their work with SWIF and validate the usefulness of SWIF with its MAC and DAC implementation. Attendees saw the value of SWIF to provide key functionality to their planning mission as well as the integration of COTS related products.

Operational Impact

The military has a number of different uses for multi-level security access, when only a select sub-group should have access to the information or the coordination of activities across agencies, with other government and non-governmental organizations. In these cases it is useful for all partners to be able to maintain control of access to their organization's data while conducting coordination and operating in a shared network space as required.

In addition to military-specific uses, Federal Emergency Management Agency (FEMA) desires to improve the whole of community response to disasters. In this case, multiple federal, state and local authorities, as well as formal and informal non-governmental organizations would need to coordinate activities. Each organization has laws, rules, regulations, mandates or operating principles that dictate the use and sharing of information. This makes it impractical for the organizations to operate in a single, shared-information space; however a distributed architecture framework such as envisioned by SWIF would facilitate this coordination, allowing organizations to share information while controlling its distribution and access.

Outside of the military, there are other communities that could also benefit from an environment with a security MAC-based framework, enabling the coordination of activities, and sharing of select company proprietary information with select partners while protecting the rest of their intellectual property from disclosure. This is especially important for institutions that are responsible for the integration of information in a single repository allowing various permutations of information sharing between organizations. It will allow different types of data to include business proprietary, educational research, and Government for official use only to be shared amongst each other or groups of people. SWIF may be the framework to enhance the sharing of different types of information seamlessly into one system to accomplish a goal or mission.

Another area where SWIF may be able to help is in the area of command and control (C2). One of the driving forces of command and control is having access to a number of C2 capabilities and data sources in order to accomplish the mission. However, depending on the access of the commander of the C2 mission, he or she may not have proper access to the important information that they may have with respect to the C2 capabilities and its associated data due to sensitivity, need to know, classification restrictions, or technology constraints. Even if the commander is given access to the information and capabilities, there exist some latency issues which may prevent the commander from getting the information in a timely manner. SWIF may be able to help with this problem by giving the commander the ability to at least be aware what C2 capabilities are inventoried for use and the communication path to contact the proper person, program, or organization on the availability and readiness of that capability. This search

capability is still under research and development by the SWIF project. However, with the SWIF framework being developed, it lends itself to develop a double blind search capability that may help with matching capabilities with mission goals.

SWIF allows for sharing of applications and information seamlessly with the DAC and MAC SWIF technical capabilities. It allows for a framework in which users are able to confidently and securely store information as well as share information on a need to know basis. It is a mechanism allowing for proprietary information from various levels to be shared in order to accomplish the mission. It may help with the question, "What capabilities do I have out there to accomplish my mission?" This SWIF capability will at least provide a means for planners and operators to know there are assets that match needed requirements in order to accomplish the mission. The awareness allows planners and operators to make that connection and with the proper access to assess the usefulness of the capability. In addition, SWIF allows for the quick integration of widgets that allows planners and operators to be able to use the information in a secure manner without jeopardizing information that a specific person does not have the need to know.

Operational Summary

The operational SWIF user receives many benefits from using the SWIF architecture including increase productivity, faster functionality, and even cost savings. Increased productivity for the users stems from SWIF enabling the user to get the right information more quickly. In particular the increased operational functionality of the SWIF to include double-blind matching web-based applications improves the user's ability match data in the database. Additionally, the interoperability of the SWIF widgets across different domains and networks allows different user to utilize the shared services, significantly decreasing the possibility of missing information due to differing classification levels.

The widget governance process also provides for faster delivery of functionality to SWIF users. The SWIF widget process uses a streamlined governance process, which embeds certification and accreditation, to shorten the delivery time. Small compact widgets, that don't impact the underlying data for the PoR, in particular have a very quick accreditation process. Even the larger widgets have a smoothly planned process for integrating into the SWIF. This decrease in delivery time allows the user to benefit from new tools and updated tools in a timely manner.

Not only does SWIF and its widgets increase productivity and deploy new tools in a smaller time frame, it also offers significant cost savings for industry, academia, and the Department of Defense. The OWF that SWIF and its widgets are based on is an open source framework allowing anyone to build their own widgets for their own specific challenges. The widgets

would still go through the governance process, but the use of the open source framework significantly reduces the barriers to entry in creating widgets. Additionally, the integration of the testing and accreditation into the widget process will reduce the maintenance needed on deployed widgets; the widgets are thoroughly tested before they are deployed, thereby reducing the errors and vulnerabilities once deployed.

Way Forward

Integration of the SWIF technology on two separate networks (high and low) will help meet the need to bridge the gap between highly classified networks and external networks, while maintaining security within a multi-level secure environment. SWIF's open architecture framework will allow for rapid deployment of analytic planning and visualization applications for the planning community while enforcing a MAC and DAC connection to a database. In addition, development of planning widgets that can retrieve row- and cell-level data from a MAC-enabled database will allow for a more granular MAC labeling that would support planning at multiple security levels.

SPAWAR
Systems Center
PACIFIC

Achieving Information Dominance: Unleashing the Ozone Widget Framework

19th International Command and Control Research Symposium
"C2 Agility: Lessons Learned from Research and Operations"
Track: 3

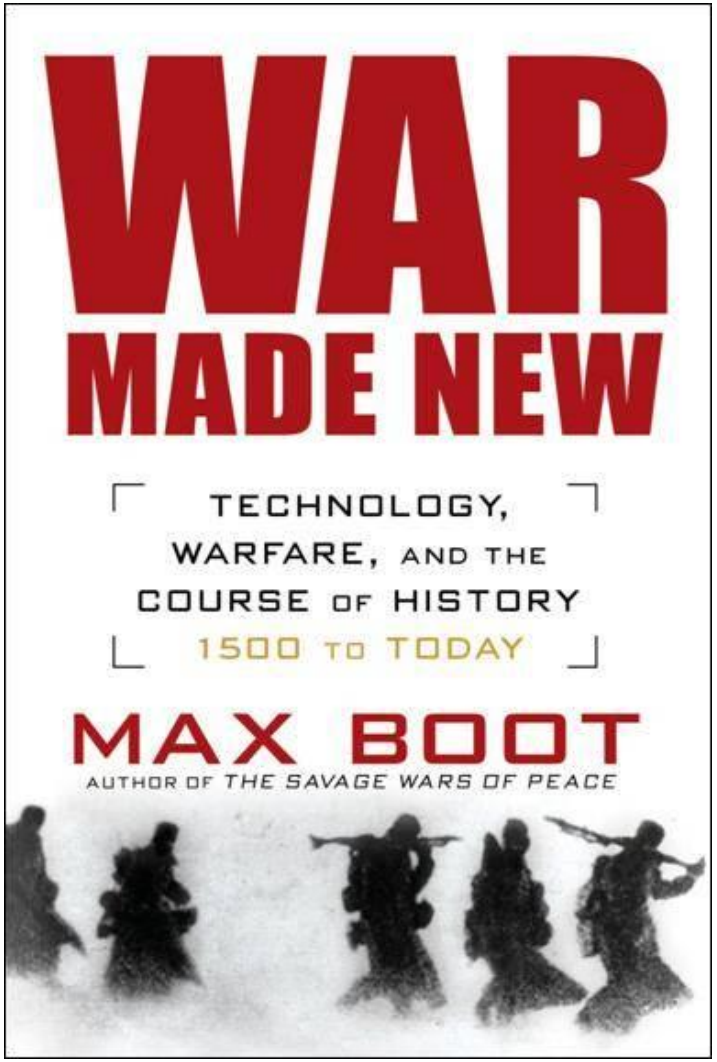
Presenters: Ms. Patty Diercks and Captain (Ret.) George Galdorisi
Co-Authors: Mr. Brent Brockman, Ms. Amanda George
Ms. Wanda Lam, Ms. Analiza Lozano
Ms. Rita Painter, Mr. Glenn Tolentino

SPAWAR Systems Center Pacific

SPAWAR
Systems Center
PACIFIC

"My view is that technology sets the parameters of the possible; it creates the potential for a military revolution."

Max Boot
War Made New



SPAWAR Systems Center PACIFIC

Overview

- Information as a Weapon
- Data Flow Issues
- SWIF Design
- SWIF Governance Process
- SWIF Widgets Demonstration
- Way Forward

SPAWAR
Systems Center
PACIFIC

Information as a Weapon

SPAWAR
Systems Center
PACIFIC

"The JIE is essential to bringing to bear the power of the Enterprise across the strategic, operational, and tactical levels. A standard, unified information environment is necessary to meet the operational and security requirements of modern joint military operations."

Enabling the Joint Information Environment (JIE)
Defense Information Systems Agency
March 6, 2014

SPAWAR Systems Center PACIFIC

The Importance of the Joint Information Environment

- From GIG…to….to…to the Joint Information Environment (JIE)
- DISA is the lead agency for JIE development
- The JCS chairman and each of the service chiefs have endorsed JIE as a military imperative
- In execution, there are three lines of operation: governance, operations, and technical synchronization
- The first increment of JIE is being implemented in Europe, the next increment to be deployed will be in the Pacific region

SPAWAR
Systems Center
PACIFIC

"Information Dominance is about warfighting. It is about warfighting in the information age."

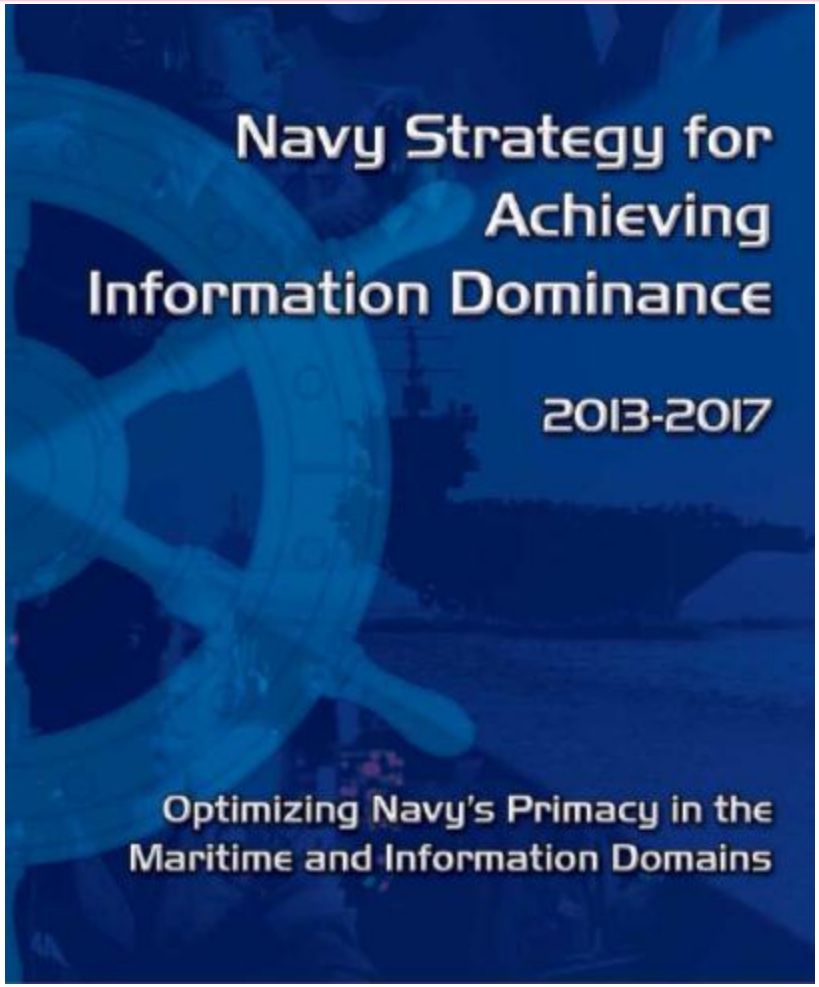
Vice Admiral Ted Branch
Deputy Chief of Naval Operations
for Information Dominance
March 6, 2014

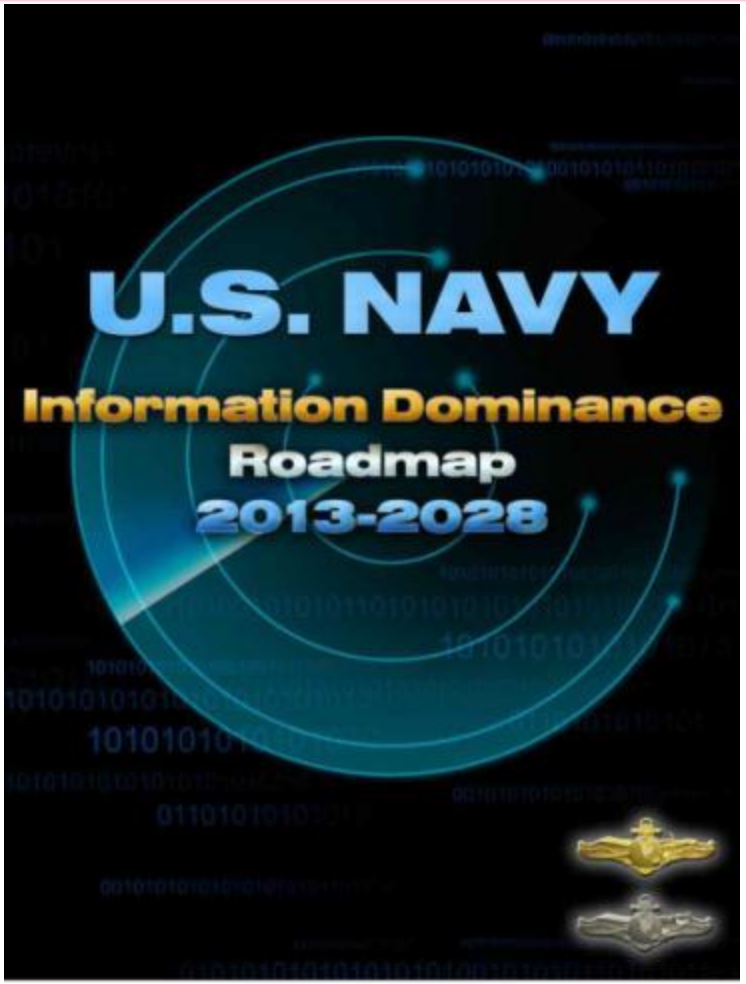
SPAWAR Systems Center PACIFIC

The U.S. Navy's Strategy for Information Dominance

- As the 1990's concept of Network Centric Warfare expanded and as technology advanced, we now have a ubiquitous network and EM spectrum from which to launch information as a weapon
- In 2009 the Navy consolidated information-related programs, resources, and manpower in order to organize, unify and concentrate its information capabilities
- Information Dominance is the operational advantage gained from integrating the Navy's information functions, capabilities & resources to optimize decision making and maximize warfighting effects
- The strategy focuses on the three fundamental Information Dominance capabilities of Assured Command and Control, Battlespace Awareness, and Integrated Fires

SPAWAR
Systems Center
PACIFIC





SPAWAR
Systems Center
PACIFIC

This all Sounds Great in Theory – but What Warfighting Challenge Does it Help Me Solve?

SPAWAR
Systems Center
PACIFIC

"In reality, the key to the pivot strategy will **not** be found in the redeployment of U.S. forces in the region or the acquisition of any particular weapons system….The heart of a successful defense strategy for the Asia-Pacific will be in the **network**."

Dr. Daniel Goure
"The Asia-Pacific Pivot Must Be About the Networks"
Lexington Institute
April 10, 2013

SPAWAR
Systems Center
PACIFIC

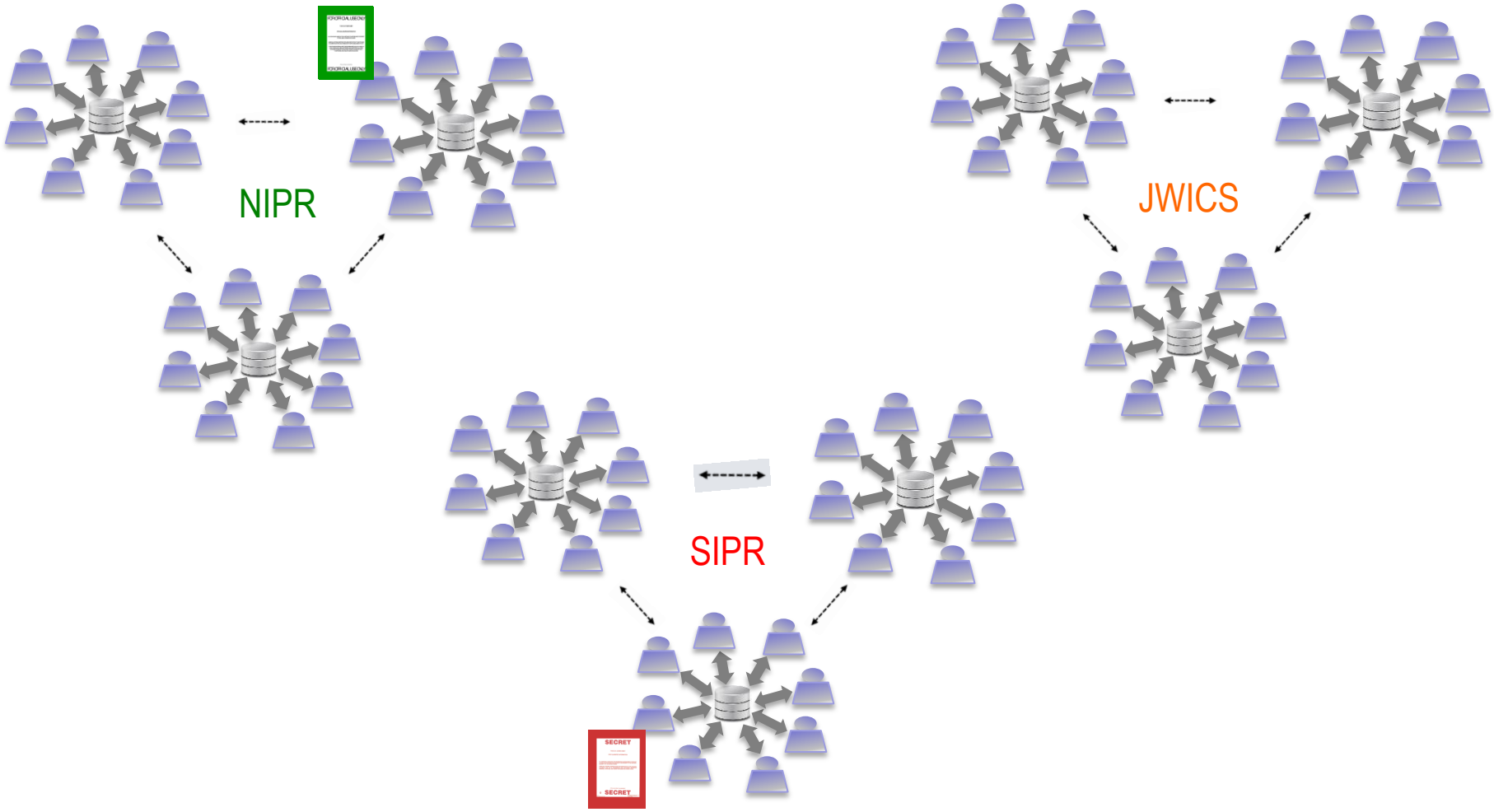
"Commanders at all levels **will require the ability to rapidly discover and access key relevant intelligence and operational data** to maintain decision superiority in contested or denied C2 environments. Such advanced capabilities involve **advanced decision support aids** that can provide real-time sharing and collaboration of authoritative intelligence and operational data across **all levels of wars**."

U.S. Navy Information Dominance Roadmap
United States Navy, Information Dominance Corps
March 2013

SPAWAR
Systems Center
PACIFIC

Data Flow Issues

Data Flow Issues – Disparate Networks



Data Flow Issues – What if…

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SPAWAR
Systems Center
PACIFIC

Secure Web Integration Framework (SWIF) Design

SPAWAR Systems Center PACIFIC

Secure Web Integration Framework

Goal:

- Provide essential information residing in multiple classification enclaves discoverable, accessible, widely shared, and understandable by the DoD community and ultimately the interagency community on both the high and low side.

Scope:

- Space and Naval Warfare Systems Center Pacific (SSC Pacific) was tasked by the Joint Staff to design an open architecture framework that allows for rapid deployment of analytical, collaborative applications in a secure and protected multi-level security environment to support a planning community.

SPAWAR Systems Center PACIFIC

System Design Considerations

- Enforcement of Mandatory Access Control (MAC)
- Data sharing via Common Data Model (CDM)
- Common User Interface (UI)
- Short application deployment time
- Web-based and lightweight client applications
- Using open source COTS/GOTS
- Application Programming Interface (API) to create MAC-enabled widgets

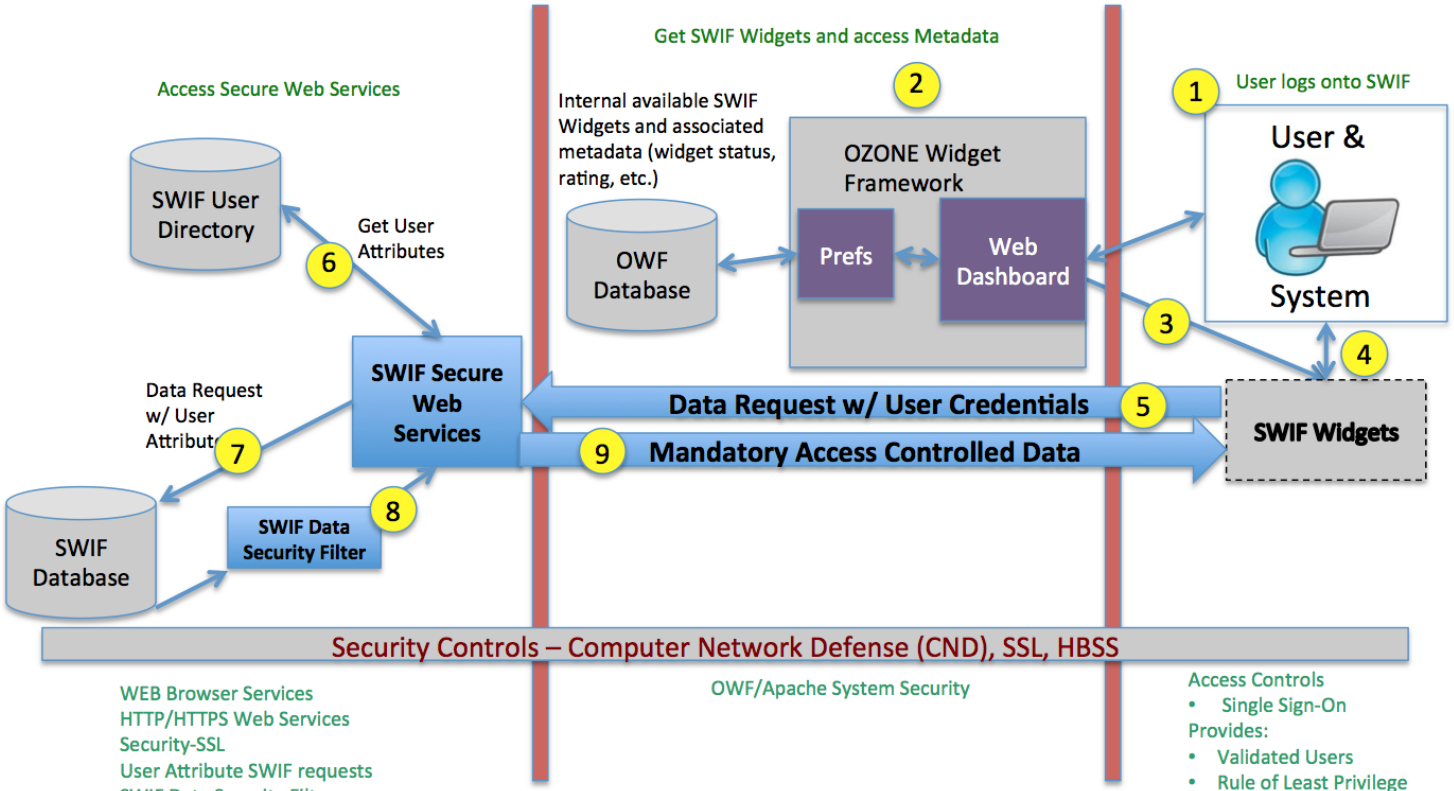
SPAWAR Systems Center PACIFIC

SWIF Components

- Presentation Framework – Ozone Widget Framework by NSA
- Custom Widgets – by SSC Pacific
- SWIF Security Service – by SSC Pacific
- Common Data Model – by SSC Pacific
- Data Source – NoSQL MongoDB

SPAWAR Systems Center PACIFIC

SWIF System



Applying APIs and Multiple Layered Security Provides DEFENSE IN DEPTH

SPAWAR
Systems Center
PACIFIC

Secure Web Integration Framework (SWIF) Governance Process

SPAWAR Systems Center PACIFIC

System Governance Process

- Complete Certification & Accreditation review of SWIF Infrastructure
- Streamline the deployment process of widgets
- Accreditation criteria based upon capabilities, complexity, and security boundaries and whether it is characterized as Simple or Medium
- Simple Widget:
  - Displays data, saves data to database, but does not communicate with other widgets
  - Limited functional & integration testing required
- Medium Widget:
  - Displays data, saves data to database, and communicates with other widgets
  - Full functional & integration testing required

SPAWAR
Systems Center
PACIFIC

Secure Web Integration Framework (SWIF) Widgets Demonstration

SPAWAR
Systems Center
PACIFIC

Secure Web Integration Framework (SWIF) Way Forward

SPAWAR Systems Center PACIFIC

Way Forward

- Integration of SWIF on high and low networks
- Certify & Accredit SWIF
- Increase functionality
- Increase data access by retrieving row- and cell-level data
- Increase data sources (e.g., file system, SQL databases)
- Explore other networks to share MAC-enabled data

SPAWAR Systems Center PACIFIC

Contact Information

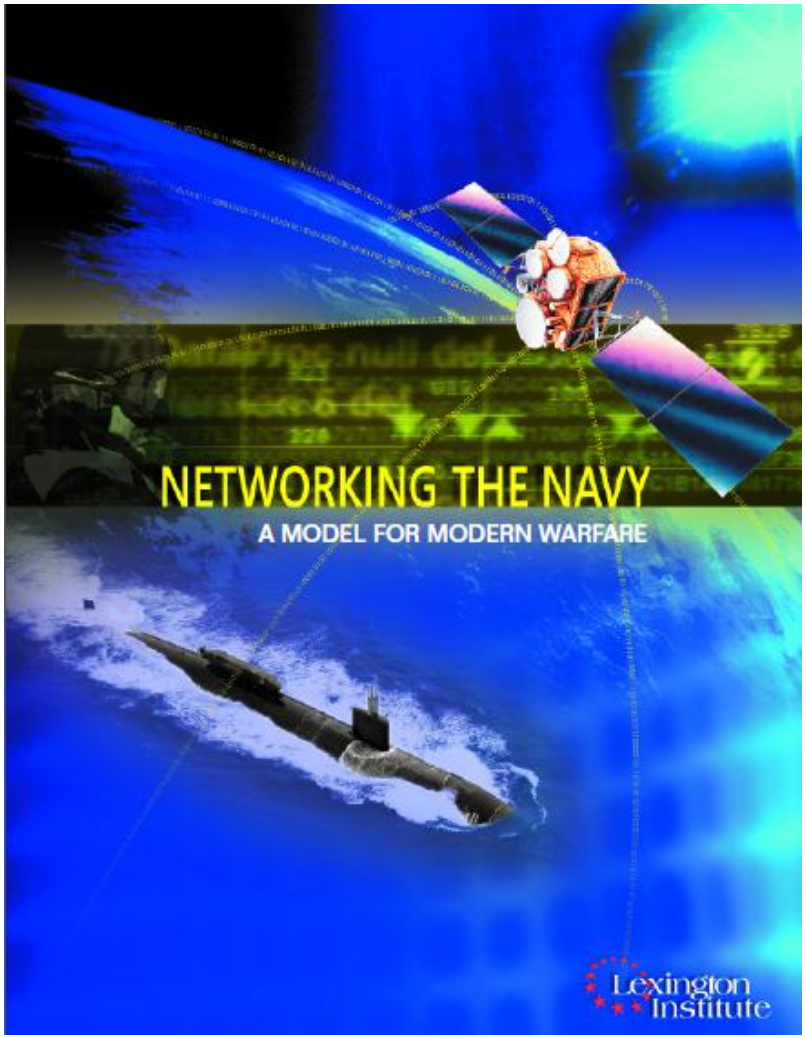
Ms. Patty Diercks
SWIF Sr. Systems Engineer
Phone: (619) 553-5159
E-mail: patty.diercks@navy.mil

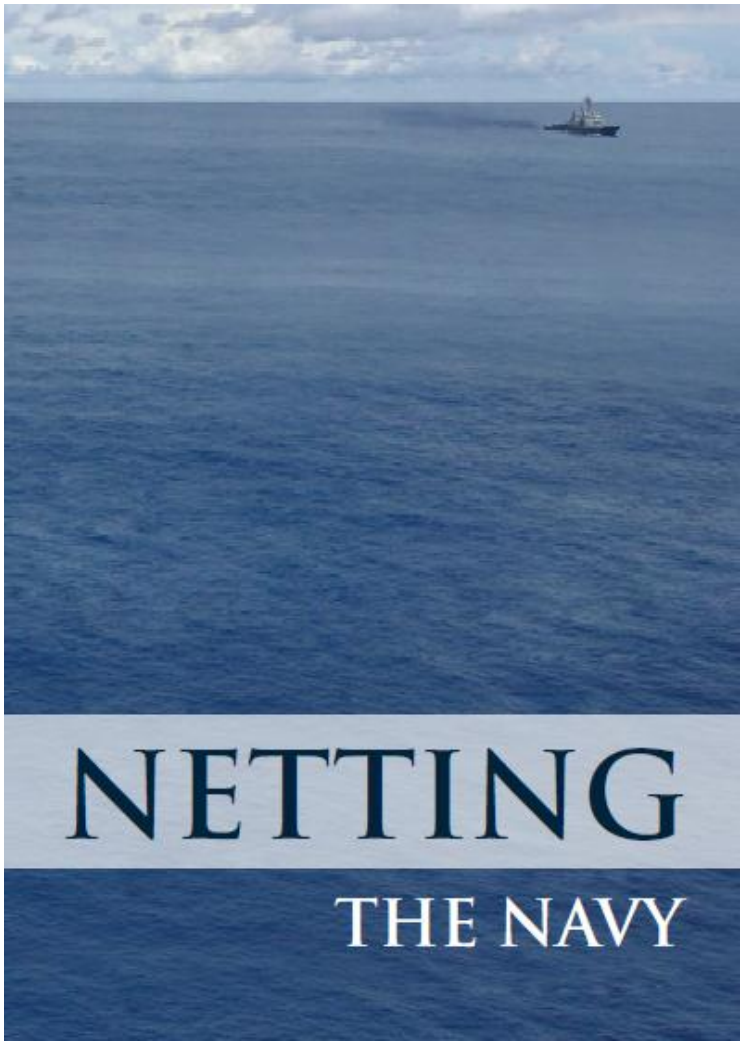
Captain (Ret.) George Galdorisi
Director, SSC Pacific Corporate Strategy Group
Phone: (619) 553-2014
Email: george.galdorisi@navy.mil

SPAWAR
Systems Center
PACIFIC

Back Up Slides

SPAWAR
Systems Center
PACIFIC





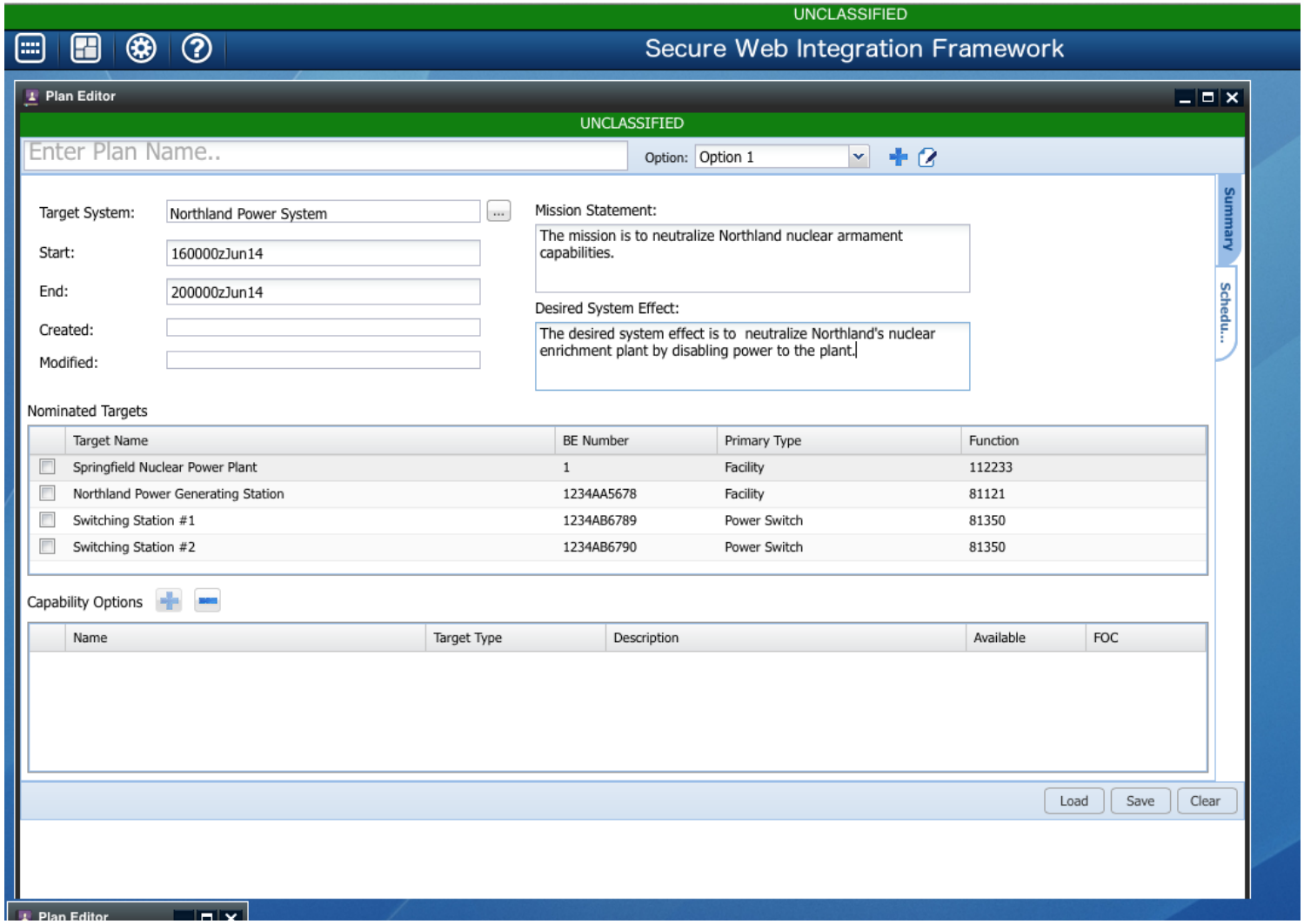
SPAWAR Systems Center PACIFIC

SWIF Widgets Demonstration

- Planning Widgets
  - Plan
  - Target Search
  - Capability Search
  - Match targets to capabilities
- Conceptual Model Visualization Widget
  - Model Search
  - Model Card
  - Data Card

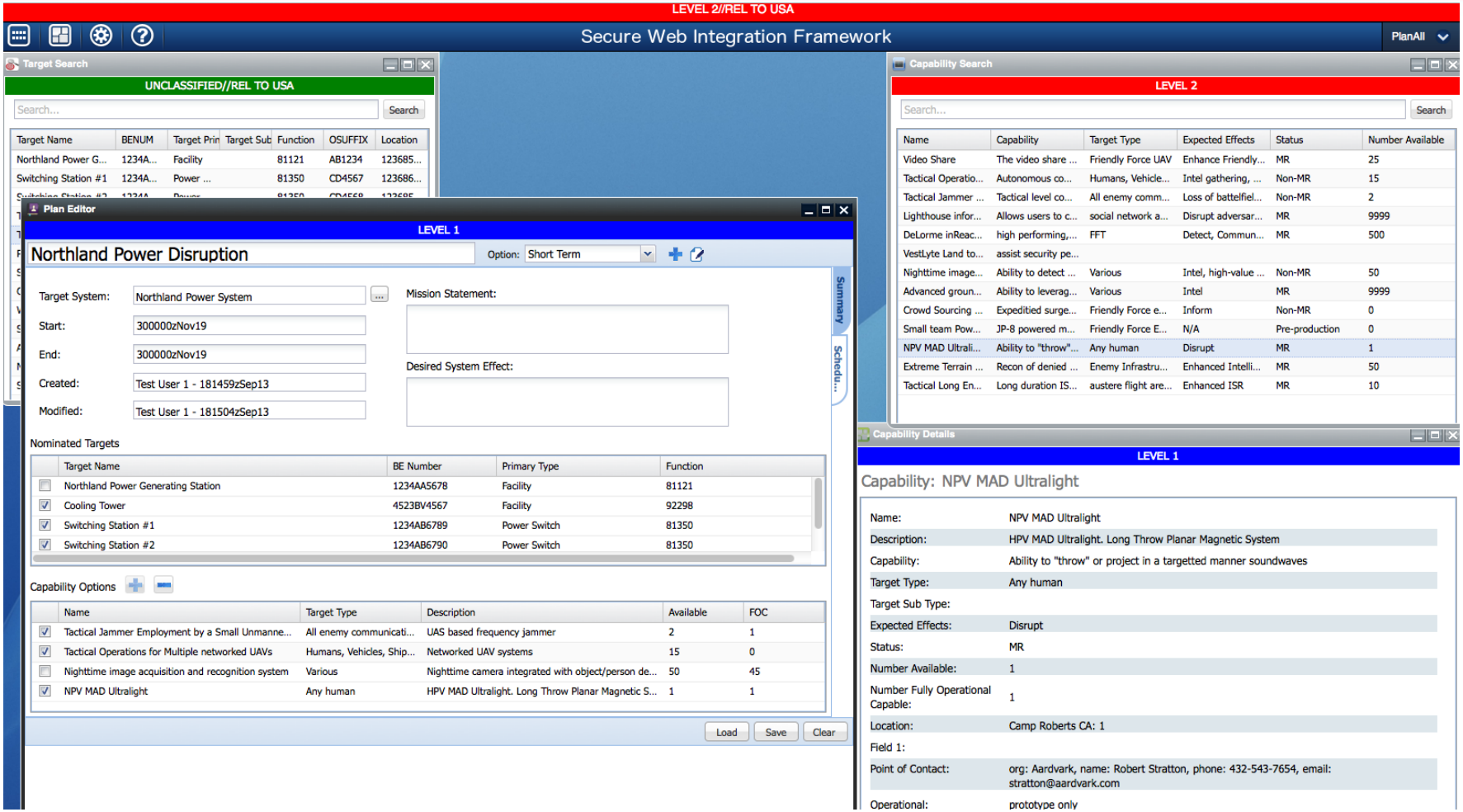
Launching SWIF (in case demo doesn't work)

Plan Edit Widget (in case demo doesn't work)



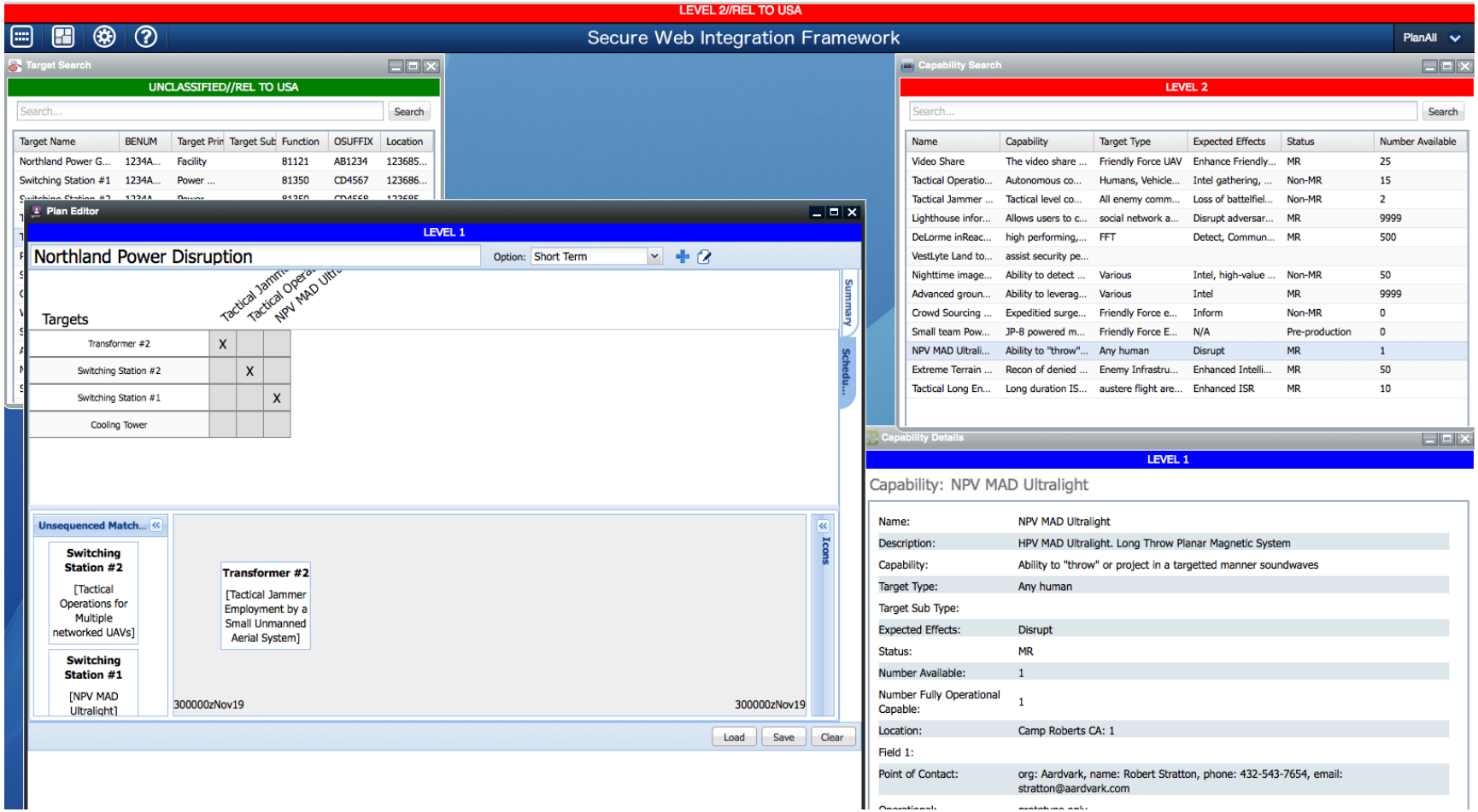
SPAWAR Systems Center PACIFIC

Widgets



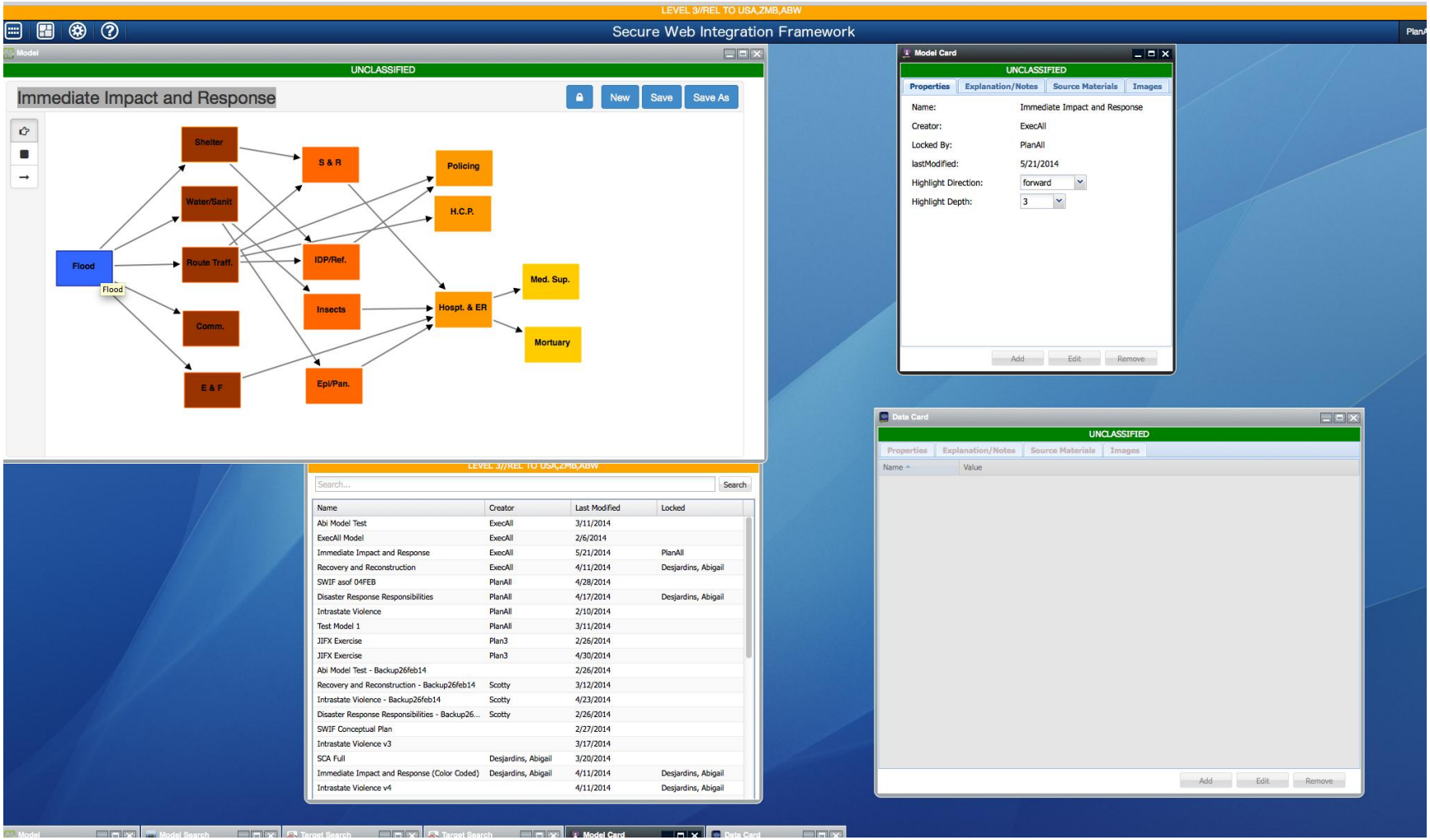
SPAWAR Systems Center PACIFIC

Widgets



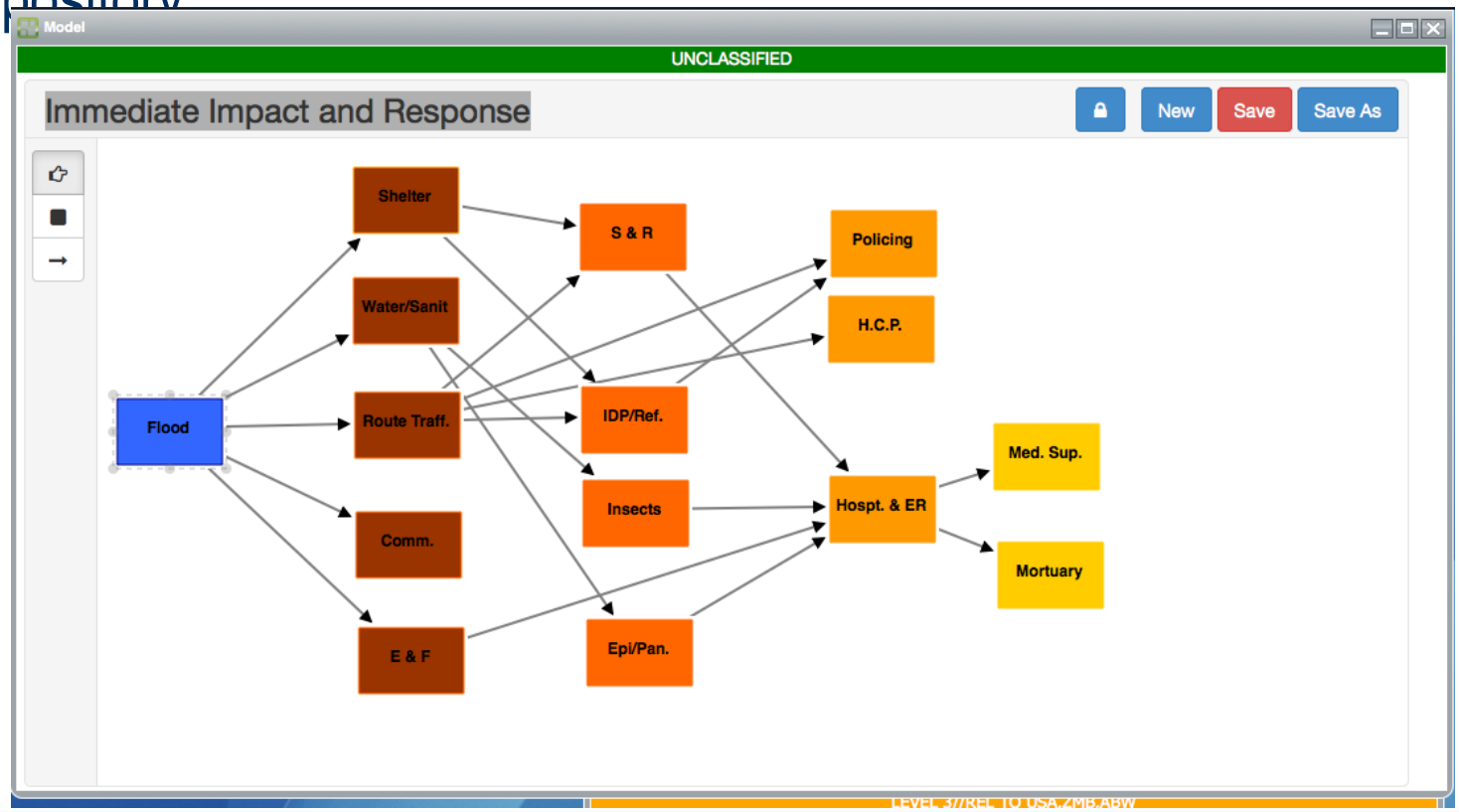
SPAWAR Systems Center PACIFIC

Widgets



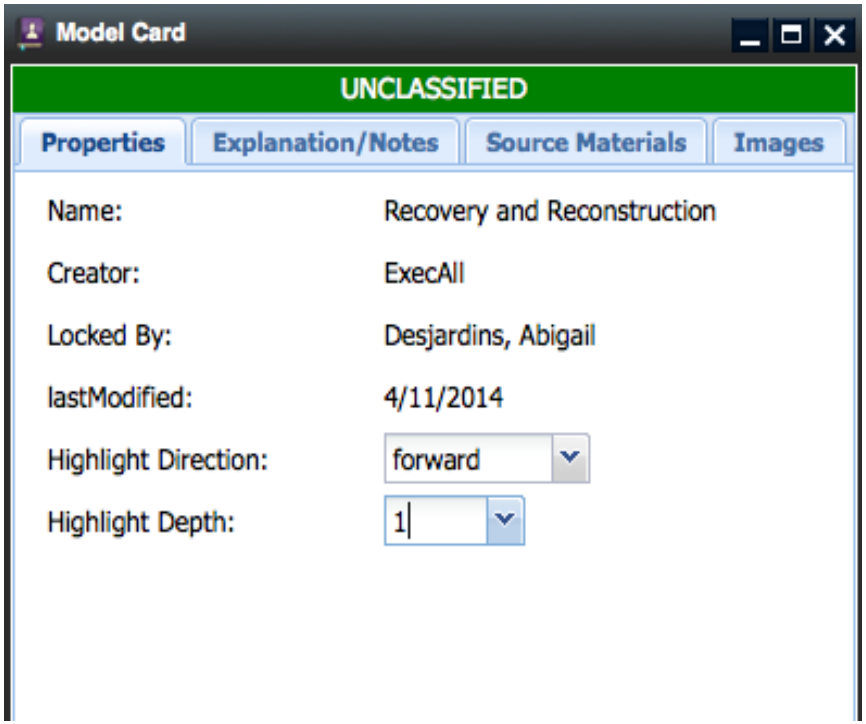
Conceptual Model Visualization (CVM) Widget

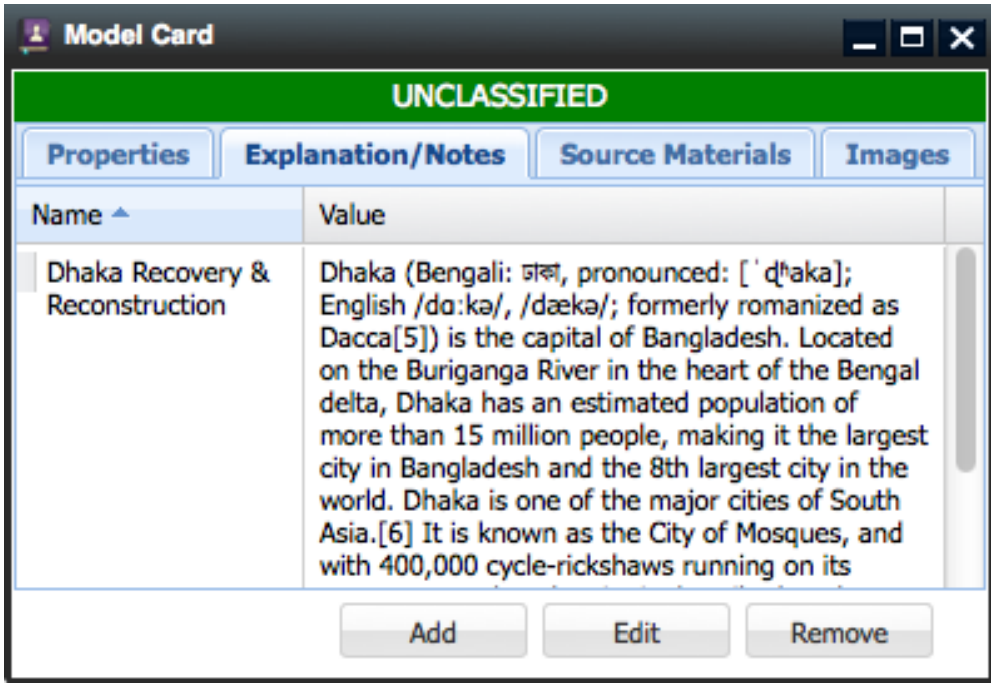
- Allows analysts to diagram relationships between Megacity infrastructures, as links and nodes, annotate nodes, attach supporting documents, and provide a security label on data saved to repository



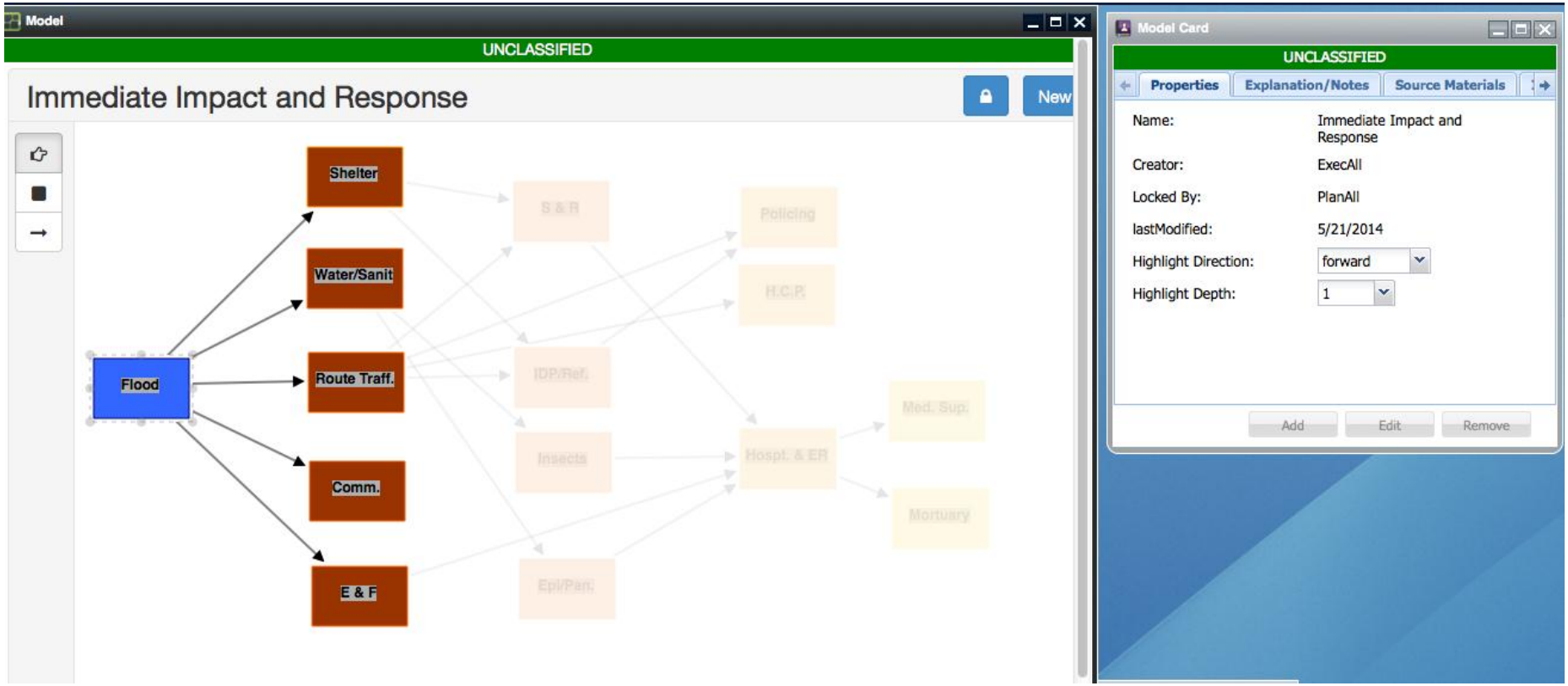
Model Card Widget – 2 Views

- View model's supporting information & configure display
  - Forwards, backwards, bidirectional, depth



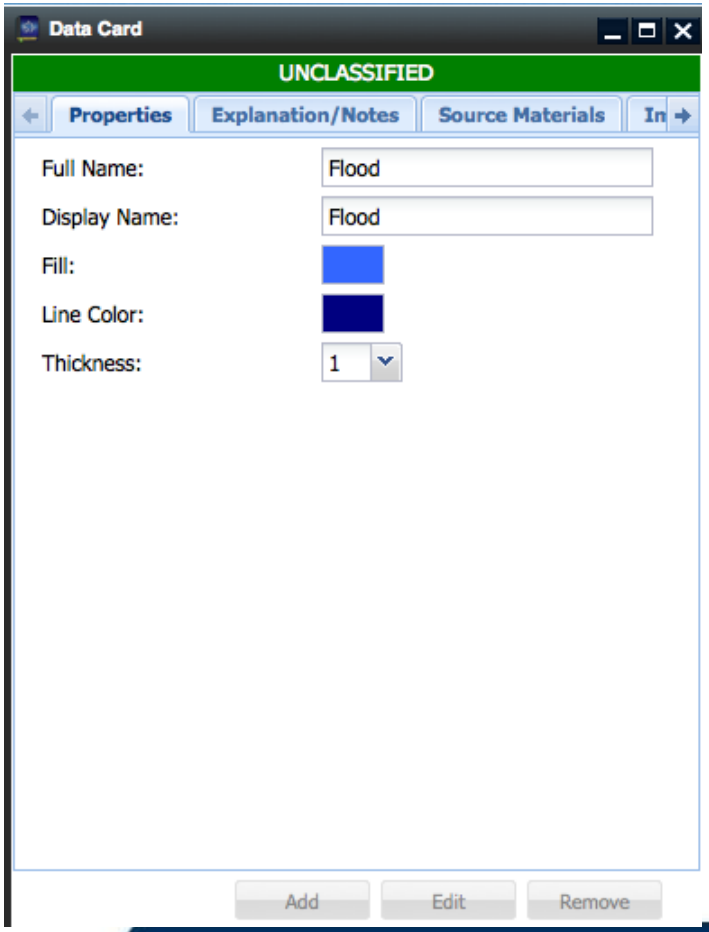


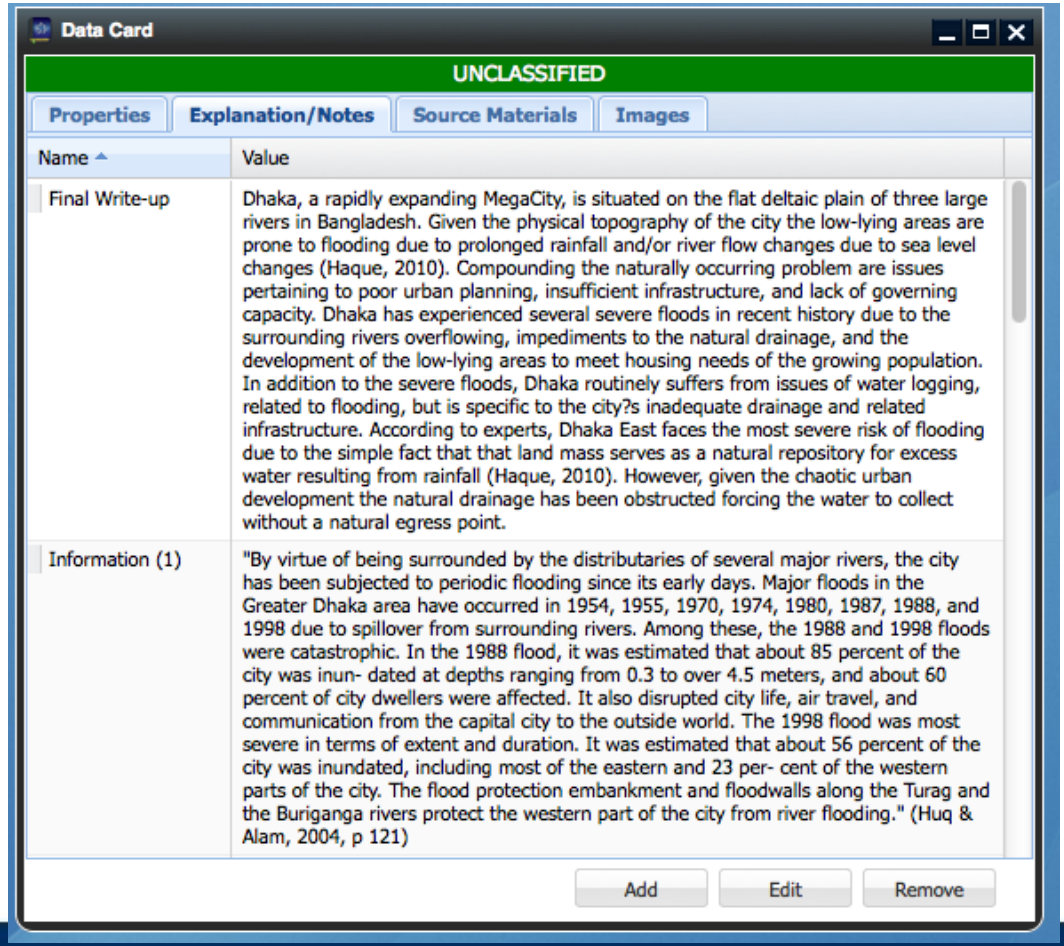
Model & Model Card Widgets



Data Card Widget – 2 Views

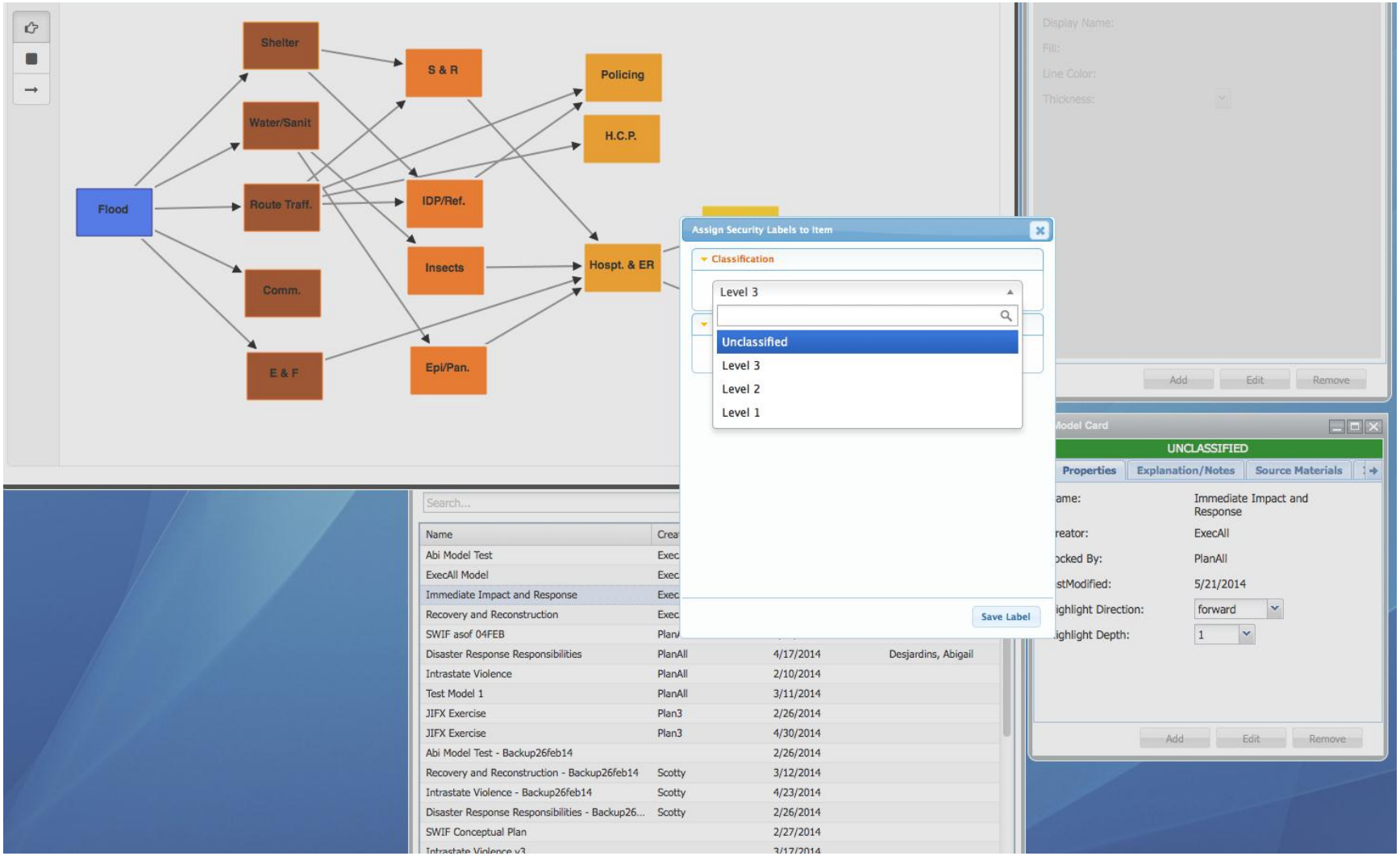
- Configuring Node Properties
- Adding Name-Value Pairs





SPAWAR Systems Center PACIFIC

Security Label



Security Label