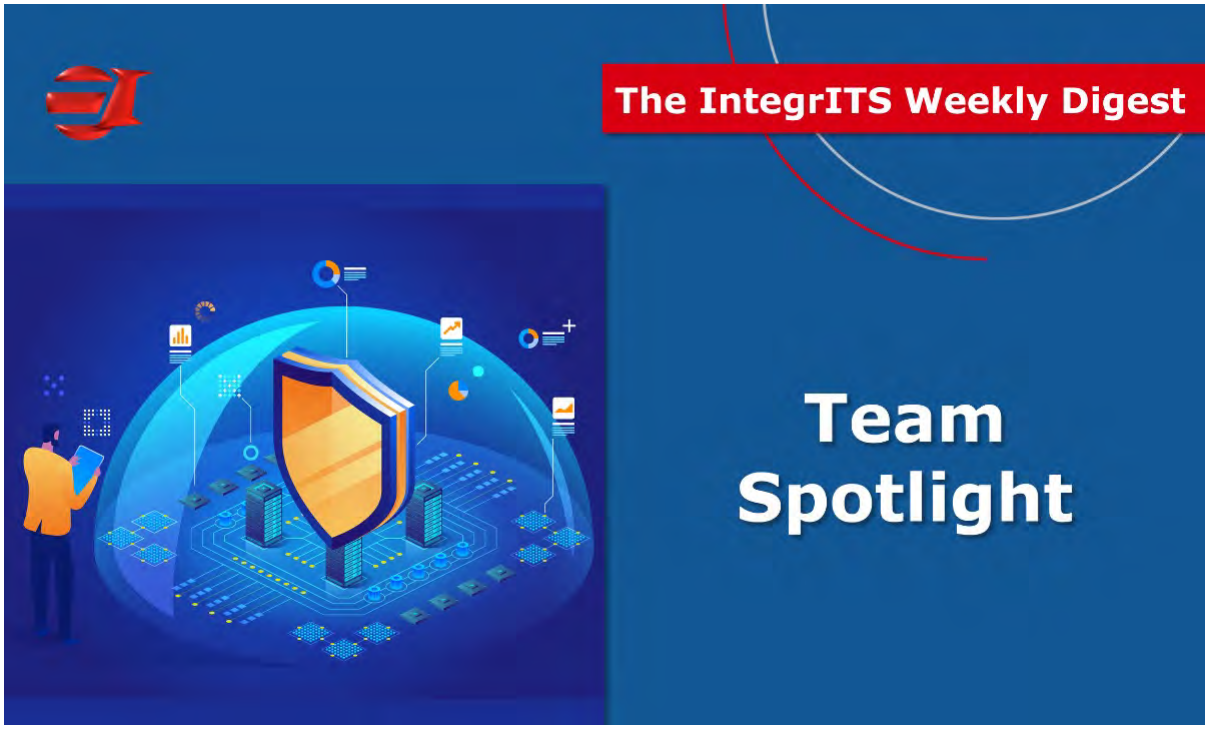


Welcome to this week's edition of *The IntegrITS Weekly Digest*!

Join us as we head to Naval Information Warfare Systems Command (NAVWAR) in San Diego and spotlight our PMW 130 Risk Management Framework (RMF) Assessment and Authorization (A&A) and Cybersecurity Team. PMW 130 may sound familiar to you because we featured another one of our IntegrITS Teams working within this Program Office back in May (the PMW 130 Professional Support Services Team).

We asked our PMW 130 RMF Team to answer a few questions about their work, but before we get into those exciting details, we thought it might be helpful to reshare information on the background of our PMW 130 work. Here's a reminder of what we shared back in May:

Background (reposted from our 05.26.22 newsletter)

For over 20 years, IntegrITS has supported NAVWAR, PEO C4I, and multiple Program Offices (PMW) responsible for acquiring fielding, and supporting C4I systems extending across Navy, joint, and coalition platforms.

One of longest standing support efforts has been in the area of Cybersecurity (CS). Our initial CS efforts were part of a Booz Allen Hamilton (BAH) Team supporting PMW 160.

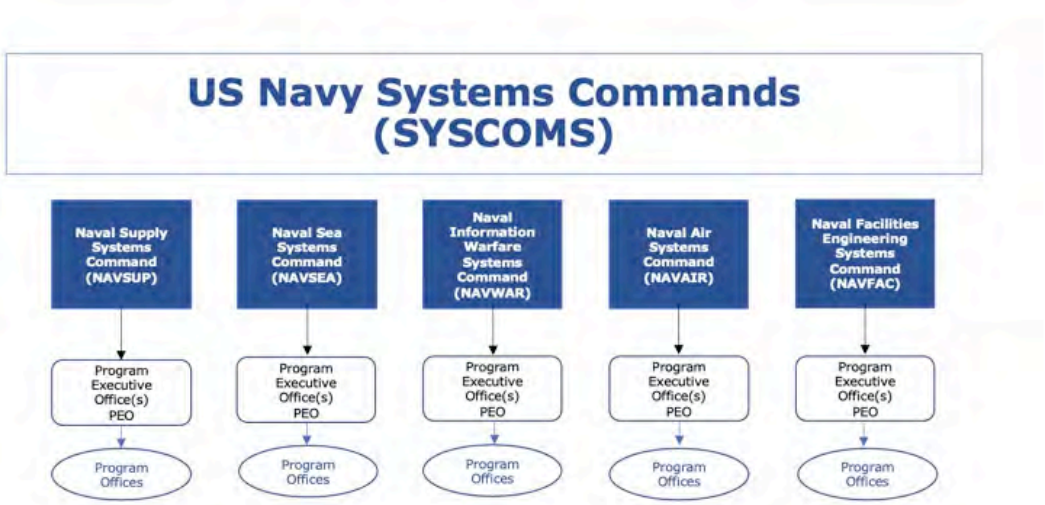
Our IntegrITS Subject Matter Experts (SME) were the authors of five volumes of the DoD's initial cyber security directives and instructions—known as the Defense Information Technology Security Certification and Accreditation Program (DITSCAP). Today this CS support effort continues, although it has transitioned from PMW 160 to PMW 130.

Our work has expanded from our initial CS policy documentation effort to IntegrITS SMEs providing Configuration Management, Logistics, and Risk Management Framework (RMF) services.

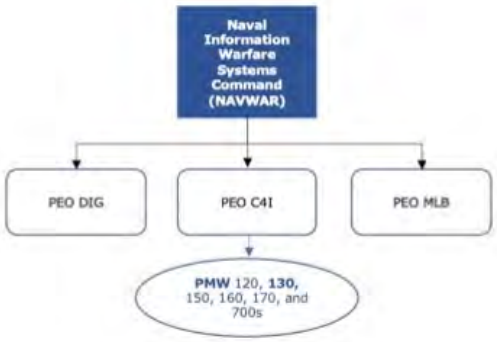
These services cover the 11 key programs and projects within PMW 130. A few examples of these programs are Computer Network Defense (CND), Navy Cryptography and Key Management, Navy PKI, Radiant Mercury, SHARKCAGE, and Vulnerability Remediation Asset Manager (VRAM).

For those outside the Navy, a little **"context"** might be helpful to understand the significance of this work effort.

The Department of the Navy has five major Systems Commands (SYSCOM), each having associated Program Executive Offices (PEO) which are made up of subservient Program Offices.



The Naval Information Warfare Systems Command (NAVWAR) in San Diego is one of these five SYSCOMS and has four PEOs, the largest is the PEO for Command, Control, Communications, Computers, and Intelligence (PEO C4I). There are 10 Program Offices within this PEO, of which PMW 130 is the Cybersecurity Program Office.



IntegrITS' PMW 130 support efforts fall under two separate contracts. One contract focuses on Risk Management Framework support (PMW 130 RMF Team). The other contract focuses on Program Office support in the areas of Configuration Management and Logistics support services (PMW 130 PSS Team).

Team Spotlight: PMW 130 Risk Management Framework (RMF) Assessment and Authorization (A&A) and Cybersecurity team

Team Members

Jason Ellis
Blesilda “Blessie” Cablayan
Rui Almazan

Location

NAVWAR | PEOC41, PMW 130
Building OT-1 and OT-2
San Diego, CA

We asked the PMW 130 RMF Team to answer a few questions about their Team and their work:

How would you describe the work your team does?

As mentioned in our explanation under "Background," PMW 130 established Navy Computer Network Defense (CND), SHARKCAGE, Navy Cyber Situational Awareness, and CND Deployer Toolkit project. These systems and services include screening, analysis, and protective services for the Outside the Continental United States (OCONUS) Navy Enterprise Network (ONE-Net), Information Technology for the 21st Century (IT-21), and Navy Cyber Defense Operations Command (NCDOC) enterprise Secure Internet Protocol Router Networks (SIPRNet) and Non-classified Internet Protocol Router Networks (NIPRNet) across the globe.

Our Team provides Security and RMF Cybersecurity Subject Matter Expert (SME) support to:

- PMW 130 Information Systems Security Managers (ISSM)
- Program Manager
- Principal Assistance Program Manager (PAPM)
- Assistant Program Manager (APM)
- Lead Engineer (LE)
- Engineering team

As a part of our work, we develop Risk Management Framework (RMF) packages in eMASS. We support ISSO and ISSM on all activities for RMF. We implement, interpret, and validate technical assessment results (Security Technical Implementation Guides (STIG) and SCANS) to achieve Authorization to Operate (ATO), Interim Authorization to Test (IATT), and Memo for the Record (MFR) authorizations. We then implement and test security controls for purposes of maintaining a systems authorization.

Our work requires that we evolve security systems by:

- monitoring the security environment
- identifying security gaps
- validating the implementation and testing of advanced STIG guidelines
- evaluating and implementing enhancements

We support the implementation of public key infrastructure (PKIs), including the use of certification authorities (CAs) and digital signatures as well as hardware and software adhering to DoD standards. When this is not possible, we assist with planned implementations of Multifactor Authentication solutions as a mitigation.

Our Team troubleshoots complex configuration problems or system issues. We conduct system security and vulnerability analyses and risk assessments and recommend the appropriate architecture/platform, identifying integration issues and procedures to apply DevOps best practices and methodologies. We perform security architecture solution trades, developing requirements for wide area networks (WANs) and local area networks (LANs), to include virtualization infrastructure, software defined networks (SDN’s) and network function virtualization (NFV), virtual private networks (VPNs), routers, firewalls, and related security and network devices.

Tell us about an accomplishment that makes your team proud.

The IntegrITS Team has a 100% success rate for ensuring that all systems under our purview are following Navy Mandates for the complete and accurate implementation of RMF and Cybersecurity directives. Our Team also ensures that the government and prime contractor are aware of any programmatic risk. We are committed to doing this in a timely manner so that a course of action (COA) can be developed quickly, and risks can be adequately managed.

We value being *proactive* as opposed to being reactive – using weekly status communications updates in meetings. Our Team operates independently with little to no input from the Customer, which demonstrates the high level of confidence they have in our work.

Out of all 40+ systems at the PMW 130 Program Office, the largest of these are managed by the IntegrITS Team.

Our team has the most experienced RMF personnel and we are often consulted for guidance by the prime contractor and government customer.

What is something you wish the whole company knew about your team?

Our Team worked together at previous environment (San Diego Navy Data Center Infrastructure – SNDCI) for a few years doing the same exact thing under DIACAP instead of RMF. Blessie and Rui were government employees (validators), and Jason was a contractor for another company. We have years of successful camaraderie under our belt, and it is one of the reasons our customers have such confidence in our work.

Tell us about any developments on the horizon in your team's area of work.

Cybersecurity and relevant products/processes are constantly evolving—and very quickly. As the Navy refines these products and processes, our Team is constantly staying abreast of the changes. We consistently seek out training and education in order to be flexible and have the ability to pivot and support these improvements.

We are working for the Cybersecurity Program Office for the entire Navy and we see firsthand the products that will be deployed to support the fleet. This includes cutting-edge classified security systems. We have a front row seat to every aspect of cybersecurity being addressed, as all of the security controls we manage cover these areas. Furthermore, the security controls we manage

are used as inputs and requirements to drive the new technologies that will be used by the Navy.

To work in cybersecurity is to work in an environment that thrives under innovation.

We are so proud of the incredible work our PMW 130 RMF Team is doing at NAVWAR. You have set a high standard of excellence with your work, and it is no wonder that our Customer has trust and confidence in the work you produce.

Jason, Blessie, and Rui, we are so grateful and honored to have you on the IntegrITS Team!

Tip of the Week

On August 9, General Michael Langley—the first Black four-star Marine general—assumed command of the U.S. Africa Command (AFRICOM). Visit this link to view last Tuesday's historic change of command ceremony held in Germany.

Coming Soon: *Operational Excellence*

Join us next week as we highlight another one of our incredible IntegrITS Teams!

Comments/Questions?

If you have any comments or questions about this week's newsletter, email us at news@integrits.com.

We have also created a website where we are storing the archives of all our newsletters to date: https://integrits.com/digest-archives/.

Have an incredible week, and we'll see you next Thursday!
Warmest Regards,
The IntegrITS Weekly Digest

Our mailing address is:
Integrits Corporation
5205 Kearny Villa Way Ste 200
San Diego, CA 92123-1420