Volume 1, Issue 2, Autumn 2018

DHS/FEMA/RESILIENCE/NPD/NTED

FEMA

TPP Times

Air Force Photo

Shifting to Data-Centric Cyber Protection Strategies

By Jared Johnson

Data is a federal agency's most important asset. As these agencies continue to strategize approaches for hardening their cybersecurity postures, safeguarding data assets warrants concentrated thought. Raw and processed data make up the most valuable asset created, owned, managed, shared, and utilized in regards to overall mission impact. However, the data protection strategies and mechanisms employed in recent years have not risen to this critical challenge.

Popular among security practitioners has been a systems-centric approach, where protection is focused on systems, hardware, networks, and other equipment that come into contact with data. However, the shift to more mobile and cloud solutions requires protections that go beyond the limitations of system-centric approaches.

Data-centric cyber protection strategies are the way of the future, and the best defense against growing advanced persistent threats (APT) in the cyber sphere.

There are four key pillars to achieving a successful strategy of data-centric security:

Data Discovery – The ability to obtain insight on what kind of data/information is stored, and where it is stored.

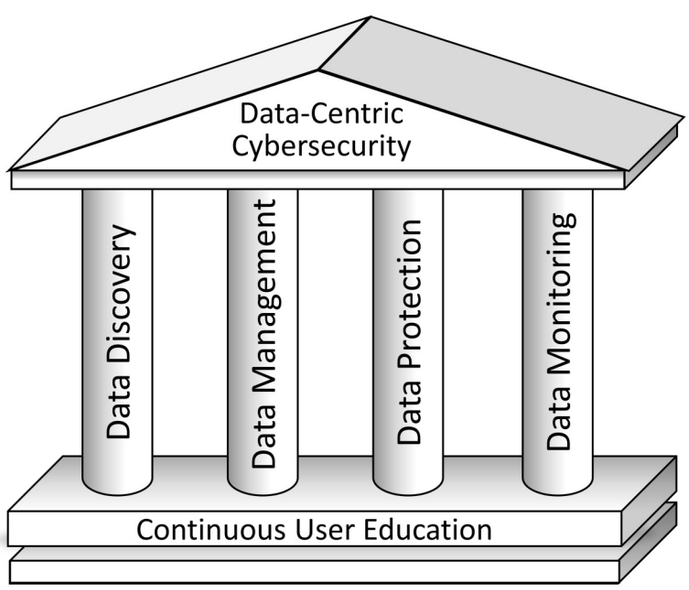
Data Management – Defining polices pertaining to data/information access which will determine which data is accessible, editable, or restricted from specific kinds of users, or locations.

Data Protection – The defense against data loss or unauthorized access of data and preventing sensitive data from being sent to unauthorized end user Person Entities (PE) or Non-Person Entities (NPE).

Data Monitoring – Continuously monitoring data access and usage to identify impactful or suspicious deviations from normal behavior.

(Continued on page 2)

Jared Johnson, CISSP CE-H, ITIL v3, has facilitated numerous cybersecurity and information assurance initiatives within the national intelligence sectors, serving the White House, Pentagon, USCYBERCOM, DHS, ODNI, Treasury, NASA, and various CONUS and OCUNUS needs of the Intelligence Community. He wrote this article exclusively for the *TPP Times*. We will regularly solicit articles from experts in emergency management to provide you with the latest insights and expertise in the field.



In This Issue

We welcome your input on the *TPP Times*, including comments, questions, and information you want to share with other Training Partners. Also let us know about additional topics you would like to see us cover, once or on a recurring basis.

Email us at tpptimes@acclaroinc.net.

(Cyber Security—Continued from page 1)

Within these four strategic pillars are key tactical data-centric elements:

Data Discovery Pillar

Data Discovery: In order to track data, it must first be located. This includes locating where the data resides, and also the networks it traverses.

Data Classification: Classifying data by type/kind and associated level of sensitivity is helpful in identifying patterns and dangerous data "hot spots"—where highly sensitive data is clustered together—in order to develop appropriate data protection strategies.

Data Tagging: Data tagging allows data to be queried quickly and efficiently. The data is "tagged" to reflect its security classification and other associated information. If individual data fields are tagged, then the IT resources that store, transmit, or process that data inherit their risk, as well as the associated controls that reduce the risk.

Data Watermarking: Data watermarking is applying classification labels and other visual markings on emails and documents to clearly display the sensitivity of the data. This in turn facilitates end user education, encouraging appropriate data handling and decreasing occurrences of unauthorized data access.

Data Management Pillar

Data Visibility: Data visibility is the process of obtaining complete visibility of data at any point, including having a history of where it has moved, where it has rested, and what transactions it has been involved in. This technique is more successful with effective data retention policies and tools in place that are complementary to the organization's business continuity and disaster recovery processes and procedures.

Data Loss and Leakage Prevention: Data loss and leakage prevention (DLP) tactics assist in protecting against data loss or intentional misuse by inside threats (hostile insider), external cyber hacking (hostile outsiders), or genuine mistakes from good-willed members of the organization (non-hostile insiders). Leakages are often revealed when data is in transit. DLP is usually most effective when incorporated in conjunction with a solid encryption and key management solution (advanced encryption standard of at least 128) and a centralized management framework designed to detect and prevent unauthorized data activity.

Data Protection Pillar

Encryption Strategies: Encryption is a data-centric protection mechanism that renders the data unintelligible and/or unusable in the case of a realized cyber exploit. With the aim of ensuring that data confidentiality remains fully intact, regardless of the location or possession of the device(s) on which it resides, encryption remains one of the most effective data-centric protection strategies. An end-to-end encryption strategy—symmetric and/or asymmetric—reduces the exploitation risks associated with the organization.

Tunneling: Tunneling (also called "port forwarding") is the transmittal of data intended for internal use only, usually through a public network, in such a way that the routing nodes of the public network are generally unaware that the transmittal is part of a private network. Tunneling is accomplished by encapsulating the internal network data and protocol information within the public network transmission units. The resulting private network protocol information then appears to the public network as data. This tunneling tactic allows the use of the public internet to convey data on behalf of an internal private network.

Data Monitoring Pillar

Identity and Access Management: When identity and access management (IAM) technologies are employed as part of data governance, managers can control user access to various levels and sensitivities of their organization's data. IAM technologies offer role-based access control, single sign-on systems, multifactor authentication, and access management. IAM technologies can also securely store profile information. IAM technologies can be used to initiate, capture, manage, and record individual user identities and their related accesses in an automated fashion.

Data Accessibility in the Cloud: The cloud environment presents additional threats, such as virtualization vulnerabilities, covert channel attacks, and misuse of cloud services. Both providers and subscribers of cloud services should ensure data is properly isolated and segregated. Subscribers should choose cloud service providers that have specific and realistic business continuity and data recovery plans in place. The plans should ensure that service can be maintained in case of a disaster and that any loss of data would be temporary and fully recovered without any degradation in confidentiality or integrity. The subscriber's own data protection and continuity plans should work in harmony with the provider's. Finally, subscribers should ensure the cloud service provider can meet their requirements for audit logs.

Continuous User Education

In the Open Systems Interconnection model (OSI), the human factor is unofficially Layer 0. Users are consistently the weakest link in any data protection strategy—and, for that matter, any cybersecurity protection strategy in general. Even the most advanced security controls can still be intentionally or accidentally bypassed by some level of human involvement. That is why continuous user education on overall security awareness at all levels of the organization is foundational to the data-centric approach.

In conclusion, combining these core pillars, and their associated tactics, results in a cyber protection strategy that focuses on the security and compliance needs of the data, and where protection layers are built out from the data itself: a data-centric approach.

Meet the Training Partners Program Team

Terry Pruitt

Terry Pruitt is the Chief of the Training Partners Program. He supervises the TPP staff and is responsible for the fiscal and programmatic oversight of the Homeland Security National Training Program. He holds a Bachelor's Degree in Criminal Justice from the University of Maryland University College and a Master's Degree in Public Administration from Central Michigan University. Terry is a retiree of the United States Air Force.

Casey Berg

NPS Photo

Casey Berg is a Program Manager who has been with the TPP for almost 8 years. His training partners portfolio includes the National Center for Disaster Preparedness at Columbia University and George Washington University, as well as serving as the CTG Program Manager. Casey is also a DHS-Certified Acquisition Professional: Contracting Officer's Representative (COR), as well as an avid traveler, hiker, and outdoorsman.

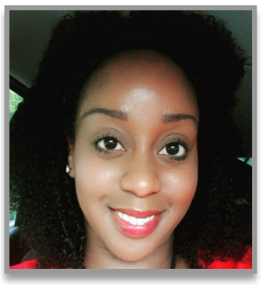
James L. Dansby

James Dansby is a Program Manager who has been with the TPP for 14 years. His training partners portfolio includes the University of Hawaii's National Disaster Preparedness Training Center and the Mission Support and Test Services, Counterterrorism Operations Support's Center for Radiological/Nuclear Training. An avid sports fan, he roots for the Chicago Cubs and the Fighting Irish of Notre Dame.

Cindy Howell

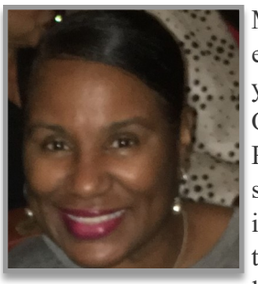
Cindy Howell is a Program Manager who has been with the TPP for 15 years, with time spent as a contractor and as a FEMA employee. Her training partners portfolio includes the Rural Domestic Preparedness Consortium, National Center for Disaster Preparedness at Columbia University, and BCFS. In addition to her work at FEMA, Cindy has owned a needlework store for several years.

Jessica E. Sterling



Jessica Sterling is a Management and Program Analyst and the newest member of the TPP Team, having joined on October 1, 2018! Her portfolio includes administrative oversight of the Homeland Security National Training Program that includes the Continuing Training Grants program and National Domestic Preparedness Consortium. Jessica is an avid painter and works on abstract paintings almost every night.

Michelle Norphlet



Michelle Norphlet is a Program Manager who has been with the TPP for 8 years. She serves as the Contracting Officer's Representative for Acclaro Research Solutions, Inc., the First Responder Training System, and the Registration and Evaluation System. Her training and education partners portfolio includes the Naval Postgraduate School/Center for Homeland Defense and Security and the Transportation Technology Center, Inc. Michelle is a FEMA Surge Capacity Force Liaison. She is also a Green Bay Packers fan.

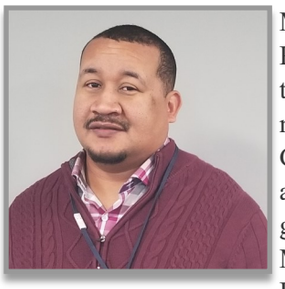
Sam Phillips

Sam Phillips is a Program Manager who has been with NTED for over 14 years, with time spent as a contractor and as a federal employee. His training partners portfolio includes the Texas A&M University, Texas Engineering Extension Service's National Emergency and Recovery Training Center, the University of Arkansas's Criminal Justice Institute, the Norwich University Applied Research Institutes, and the University of Texas at San Antonio. Sam has lived in six American states, as well as Germany and Belgium. He is an avid sports fan.

Willie Johnson, Jr.

Willie Johnson, Jr. is a Program Manager and Training Specialist who has been with the TPP for 14 years. His training partners portfolio includes Louisiana State University's National Center for Biomedical Research and Training (NCBRT), University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism, and the Virginia Center for Policing Innovations. Willie loves to fish, play chess, and cheer for the Dallas Cowboys.

Micheal Anthony Scott



Micheal Anthony Scott is a Training Program Manager who has been with the TPP for 5 years. His training partners portfolio includes Frederick Community College, the International Association of Firefighters, Georgia Tech Research Institute, and New Mexico Tech's Energetic Materials Research and Testing Center. Micheal is a Houston Texans fan and likes to attend their away games.

Did You Know?

Molly Williams was the first known female firefighter in the United States. While a slave, she volunteered for the Oceanus Engine Company #11 in 1815 and fought fires in a dress and apron.

FEMA Photo by Andre R. Aragon

The Importance of the PDF Tag Tree

From the Editors

This year marks the 25th birthday of the Portable Document Format, better known as the PDF. Adobe Systems introduced the PDF in 1993 into a computing world that resembled the wild west, one with a slew of competing proprietary—and incompatible—software and hardware standards. The PDF was designed to allow documents to appear the way their designers intended, regardless of hardware or software. Take a second to appreciate that this is actually pretty remarkable even today—try uploading a Word document to Google Docs, for example, or opening a spreadsheet on your phone.

Because of the way the file is built, the PDF is an ideal format for making documents accessible to users with disabilities, allowing parts of the document like paragraphs, headings, and images to be extracted and used by assistive technology, like screen readers. For this to work, however, the PDF needs to be correctly tagged.

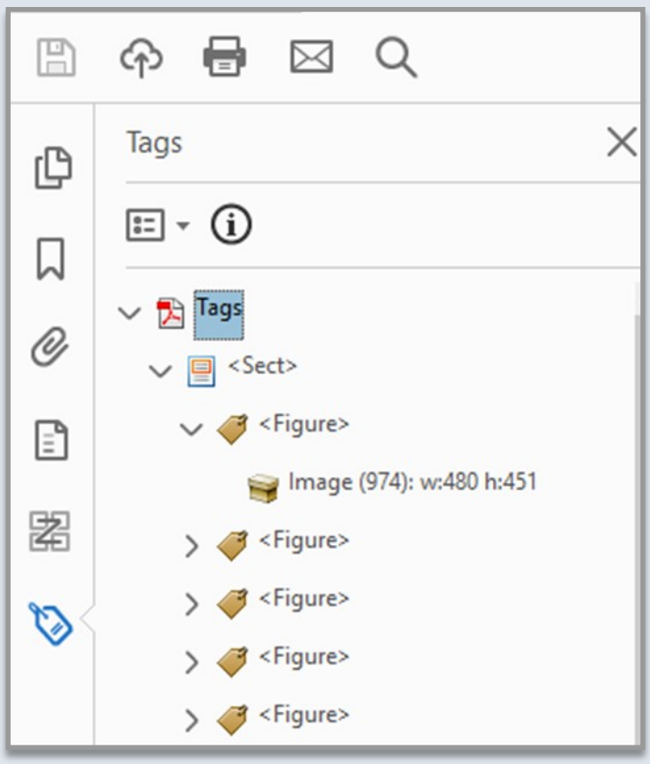
Tags in a PDF are used to identify the content, telling the computer what each piece of content is. The tags are contained in the tag tree. The tag tree is like the outline of the document and thinking of it in this way will help you understand how tagging impacts accessibility.

The tag tree can be accessed from Acrobat's left-hand navigation bar (note that you'll need the full version of Acrobat; the free Reader does not allow editing), opening the Tags pane. The Tags pane shows every tag in the document vertically from first to last. Note that tags may be nested under other tags—again, like an outline—and that most entries on the tag tree can be expanded, showing all of the tags underneath.

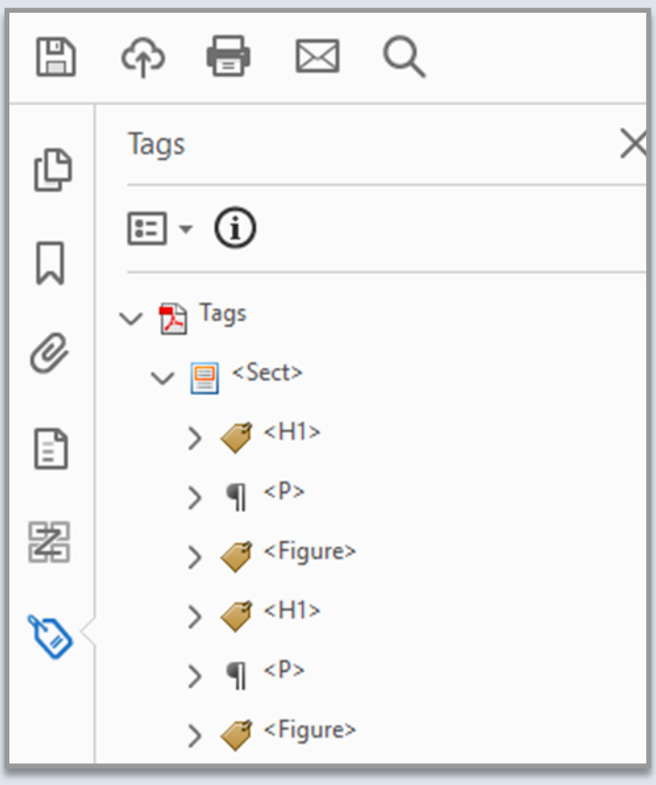
Right clicking on a tag will bring up a context menu with a variety of options—one option that you'll want to toggle on is "Highlight Content"; this function will bring you to the actual content in the document that the tag represents. You can also select "Properties" to open the tag's Object Properties window. Here you'll be able to change the tag type (for example, make Paragraph text into Heading Level 1 text), as well as add alternate text; alternate text is read by assistive technology instead of the actual content—this is almost always used for Figures, but can be applied to any type of tag.

Within the tag tree you can drag and drop tags to change their order or change how they are nested. This is important because, like an outline, the tag tree should follow the linear order of the document. Depending on how you create your PDF the tags may be in the correct order already; however, because different programs layer documents in different ways (and different PDF generators process those layers in different ways) you may see tags ordered incorrectly or grouped in strange ways. Because assistive technology uses the tag tree to understand the document, it's important to ensure that the tag tree is clean and free of unnecessary or incorrect tags and follows the document's logical reading order.

Accessibility may not have been in mind when the PDF format was rolled out to standardize document presentation, but its architecture made it a key platform for accessibility, ensuring that all users can access a document's content in a standard way.



The tags pane, shown above, can be accessed by clicking the tag icon in the left-hand navigation. Tags with a right chevron can be expanded. You'll see the first <Figure> tag has been expanded to show its contents (page content is represented by the box icon). Notice all of this document's images appear first in the tag tree as <Figure> tags—this is incorrect in this case, because it doesn't match the order of the document. A correct order would match the way the page should be read—which in this case is heading first, then page text, and then the image:



Find more resources at: https://section508.gov/create

Welcome Back to Scott Kelberg

From the Editors

The TPP would like to welcome back Mr. Scott Kelberg, who is returning to NTED after a year away serving as a Fellow in the White House Leadership Development (WHLD) Program. Scott was accepted into the third cohort of this program, after being personally recommended by the Deputy Secretary of Homeland Security, Elaine C. Duke. He competed with a number of other nominees through several rounds of interviews, and was ultimately chosen as one of fourteen program fellows, a cohort made up of GS-15 level Federal employees.

The WHLD Program, sponsored by Executive Office of the President (EOP) and supported by the President's Management Council (PMC) and the Performance Improvement Council (PIC), provides a unique growth opportunity focused on developing high-potential career GS-15s and equivalents poised to enter the next generation of career senior executives. Participants work on the Federal government's highest priority and highest impact challenges that require the coordination of multiple Federal agencies to succeed.

"Essentially, you are parachuted into a completely new environment," Scott said. "You don't know anyone. You don't have the expertise. But you show off your moxie: you have to be adaptable and flexible enough to dive right in and manage a government-wide program you've never even heard of."

> "You show off your moxie: you have to be adaptable and flexible enough to dive right in."

The WHLD Program places cohort members in either the Office of Management and Budget (OMB) or the General Services Administration (GSA). The major focus for the fellows is supporting 15 cross-government initiatives related to the President's Management Agenda (PMA) in areas such as technology, grants, performance, customer experience and engagement, and more.

Scott was embedded with the GSA from September 2017 until September 2018, supporting a wide breadth of tasks, including working inside of cross-government councils geared toward the development and implementation of PMA goals, and GSA -specific projects, such as a government-wide customer satisfaction survey about mission support services in each agency.

The yearlong WHLD Program is a three-pronged engagement. Fellows led the development of PMA items, worked on ancillary projects at their location, and met with each other on Fridays for weekly development. Scott said, "These development sessions were the highlight of each week. There was bonding over the similar thoughts and emotions we were having. It's nice to have that at that stage of your career." Other highlights for Scott included touring both the East Wing and West Wing and visiting the CIA. "It's something I'll never forget," he said of the CIA tour, which included discussions with a panel of SES's and a tour of the CIA Museum.

Now that he is back in the NTED offices, Scott is excited to

put the lessons he learned to work for FEMA. "Adaptability is probably the biggest lesson—but that's one of those things you learn at FEMA anyway," Scott said. "It was so many different types of jobs in one. I would go from the duties of someone at an SES level to GS-7-level work. Your teammates lean on you; they just assume you can get the job done. It was very humbling." He said the WHLD taught him to be flexible, and caused him to have to refresh old skill sets that he once used, but had become stale.

Scott's goals include creating strategic plans for NTED initiatives based on private sector examples, geared at saving money. "I want to preach efficiencies and shared services. Where can we share, instead of everyone doing their own thing?" Scott says he wants to eliminate waste, make NTED as efficient as possible, and think just as much about the taxpayer as about the first responder.

Scott manages over $120M annually in nationwide training and education programs, to include the National Domestic Preparedness Consortium and the Center for Homeland Defense and Security. He previously served as the Senior Advisor to the Director at the Nationwide Suspicious Activity Reporting Program Management Office at the Department of Justice, with responsibility for the development and implementation of training programs for law enforcement and intelligence analysts. He is also a graduate of FEMA's Pinnacle Program—an opportunity for GS-15 employees to build proficiency in mission critical leader competencies, while taking challenging classes through the American University's Key Executive Program.

Since his return in early October, Scott is serving as the Acting Director of NTED, a promotion from his previous position of Assistant Director.

NTED Course Updates: New, Revised, Recertified, and Retired

From the Editors

New

- AWR-365-W Countering Violent Extremist Narratives, University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism
- AWR-310 Natural Disaster Awareness for Community Leaders, University of Hawaii, National Disaster Preparedness Training Center
- PER-365 Emergency Response to HazMats, International Association of Fire Fighters
- PER-332 Population Monitoring at Community Reception Centers, Counterterrorism Operations Support
- PER-351 Preventive Radiological/Nuclear Detection Team Leader, Counterterrorism Operations Support
- PER-347 Personal Protective Equipment—Mission Specific Competencies, Counterterrorism Operations Support
- PER-371: Cybersecurity Incident Response for IT Personnel, University of Arkansas, Criminal Justice Institute

Revised

- None

Recertified

- AWR-187-W Terrorism and WMD Awareness in the Workplace, Rural Domestic Preparedness Consortium
- AWR-302 Pipeline Security for Rural Communities, Rural Domestic Preparedness Consortium
- AWR-314-W: Medical Countermeasures Awareness for Public Health Emergencies, Texas Engineering Extension Service
- AWR-173-W: Information Security Basics, Texas Engineering Extension
- AWR-174-W: Cyber Ethics, Texas Engineering Extension Service
- MGT-318 Public Information in an All-Hazards Incident, Texas Engineering Extension Service
- MGT-415 Disaster Recovery in Rural Communities, Rural Domestic Preparedness Consortium
- MGT-315: Critical Asset Risk Management, Texas Engineering Extension Service

The National Integration Center advised that an additional 28 NIMS curriculum courses are in final revisions for NIMS 2017 and will be available as they are completed and approved for release.

Retired

- None

NIMS Alerts

From the Editors

These alerts provide important information on new NIMS guidance, tools, and other resources. For your convenience each alert is a hyperlink you can click that will bring you directly to the appropriate webpage.

- NIMS Alert 26-18: Publication: NIMS/NQS Emergency Operations Center Skillsets
- NIMS Alert 25-18: FEMA Releases Vance Taylor's Prep-Talk: "We Succeed or Fail Together!"
- NIMS Alert 24-18: National Engagement Period: National Qualification System (NQS) Supporting Tools
- NIMS Alert 23-18: FEMA Seeks Feedback on Planning Considerations: Evacuation and Shelter-In-Place
- NIMS Alert 22-18: FEMA Releases Planning Considerations: Complex Coordinated Terrorist Attacks
- NIMS Alert 21-18: FEMA and Emergency Manager Partners Release School Safety PrepTalks
- NIMS Alert 20-18: FEMA Releases Revised IS-2900.a Course
- NIMS Alert 18-18: FEMA Releases Revised IS-100.c and IS-700.b Courses

NIMS Alert 20-18 and 18-18 indicated that the Emergency Management Institute (EMI) recently released three revised online NIMS courses:

- IS-100.c An Introduction to the Incident Command System, Emergency Management Institute. ICS-100 introduces the Incident Command System (ICS) and provides the foundation for higher level ICS training.
- IS-700.b An Introduction to the National Incident Management System, Emergency Management Institute. IS-700.b is an overview providing learners with a basic understanding of NIMS concepts, principles, and components.
- IS-2900.a National Disaster Recovery Framework (NDRF) Overview, Emergency Management Institute. The NDRF Overview course provides an introduction to the NDRF and establishes a common platform and forum for how the whole community builds, sustains, and coordinates delivery of recovery capabilities. The NDRF provides individuals supporting disaster recovery efforts with a foundation in NDRF key concepts, guiding principles, and roles and responsibilities of NDRF leadership.

The National Integration Center advised that an additional 28 NIMS curriculum courses are in final revisions for NIMS 2017 and will be available as they are completed and approved for release.

Upcoming Events

From the Editors

Community Disaster Resiliency Network (CDRN) Training Summit

- **Dates**: November 19, 2018
- **Location**: Kansas City, KS

NDPC & CTG Annual Kick-Off Meeting

- **Dates**: January 9 – 10, 2019
- **Location**: Washington, DC

Questions, comments, or story ideas
for the *TPP Times*?

Email tpptimes@acclaroinc.net

www.firstrespondertraining.gov