SENIOR LEADER PERSPECTIVE: DR. ERNEST MCDUFFIE, LEAD FOR THE NATIONAL INITIATIVE FOR CYBERSPACE EDUCATION (NICE)

NSCI's Charles Winstead recently had the opportunity to interview Dr. Ernest McDuffie who is currently the Lead for the National Initiative for Cybersecurity Education (NICE). Prior to NICE, he was appointed Associate Director of the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD) in February 2008. From early September 2009 until early November 2009 he served as Acting Director of the NCO. His appointment as the Associate Director of the NCO comes after joining the NIST as a Computer Scientist in their Information Technology Laboratory, Office of Federal and Industrial Relations. In August 2006, Dr. McDuffie joined the NCO where he served as the Technical Coordinator for the Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG), Federal Agency Administration of Science and Technology Education and Research (FASTER) Committee of Practice (CoP), and the Software Design and Productivity (SDP) Coordination Group (CG). Dr. McDuffie received his Ph.D. and M.S. degrees in Computer Science from the Florida Institute of Technology in Melbourne, Florida.

NSCI: Can you tell us a little bit about the National Initiative for Cybersecurity Education (NICE), who is involved, and your priorities for 2011 and beyond?

MCDUFFIE: NICE is the extension of CNCI-8 which was the education part of the Comprehensive National Cybersecurity Initiative started under the previous administration. We are currently busy planning for the expansion from a federally focused to a national initiative. Key agencies involved are DHS, NSF, DoD, ODNI, Department of Education, OPM, and NIST as the agency lead and coordinator. We are currently involved in a major Strategic Plan development process which will identify priorities for 2011 and beyond.

NSCI: After approximately one year leading NICE, are there any successes you would like to highlight?

MCDUFFIE: The kick-off workshop held in August of 2010 at NIST headquarters in Maryland was a big success with about 200 people in attendance representing academia, private industry, and Federal agencies. A high level overview of what we envision NICE to be all about was presented. A number of grass roots efforts were initiated by several different groups. These efforts are an important component of our dual goal of enabling top-down and bottom-up efforts across multiple communities in order to

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 1**

achieve the comprehensive education, training, awareness, and professional development goals set for NICE.

NSCI: In 2010, NICE was expanded from a federal to a national focus. How has that changed the initiative?

MCDUFFIE: It dramatically increased the scope and changed the focus to a truly national comprehensive effort that will ultimately affect the entire country in terms of everything from improved awareness, to increased job opportunities in a better-defined cybersecurity workforce, to enhanced cybersecurity for the country's critical infrastructure.

NSCI: Numerous academic institutions have ramped up their cyber-related programs for undergraduate and graduate students. But how do you think we are doing in terms of reaching the casual internet user?
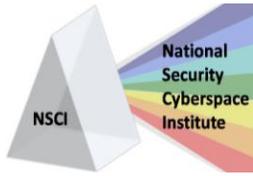
MCDUFFIE: To answer this question in a meaningful way requires first defining and then base-lining of that particular population, "the average/casual internet user." It will be interesting to discover exactly what the definition of the average internet user turns out to be and then to actually measure how well we are reaching them in terms of modifying their behavior in a positive direction. This is a fundamental goal of NICE.

NSCI: Small businesses typically lack the resources available to large organizations, especially when it comes to an infrastructure to support cybersecurity. Given small businesses are a key source of research and innovation, do you have any ideas on how we can improve their awareness of cybersecurity threats, vulnerabilities, risks, and solutions?

MCDUFFIE: Providing a portal where all can access information that can be used to improve their cyber hygiene in all of these areas is also a goal of NICE. Through NIST-established relationships with small business we will be able to identify informational needs specific to their sectors and size of operations. Every component of the population will have slightly different informational needs which must be addressed for NICE to succeed.

NSCI: Are there any particular metrics associated with NICE that let you know how the initiative is affecting cybersecurity awareness, recruitment, education and training?

MCDUFFIE: Metrics are key to measuring progress, and developing the correct metrics is a non-trivial activity. Cybersecurity metrics are particularly difficult because of the relative newness of the field and its dynamic nature. Each area asked about in this question will require a separate set of metrics specifically designed to measure the most important aspects of that area. We will be working with subject matter experts, private sector, and academic stakeholders to determine the most meaningful and collectible metrics for each area as part of the baselining for those areas so that programs designed to impact them will know what metrics to collect and be designed in such a way as to facilitate that process.

110 Royal Aberdeen ⬤ Smithfield, VA 23430 ⬤ ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 2**

NSCI: So how do you think we are doing with metric identification and collection thus far? Any estimate on when something might be available?

MCDUFFIE: Some programs are collecting meaningful metrics, the Federal Cyber Service: Scholarship for Service program is an example. However, the broad goals of NICE will require in addition to the aggregation of existing metrics the development of new metrics specific to our broader goals. We are at the beginning of the process to identify exactly what the best set of such metrics will be as we design and implement new components of NICE.

NSCI: NICE is obviously an initiative that creates jobs and a future workforce that will be competitive internationally. How is NICE's budget doing given the current economic climate?

MCDUFFIE: Job creation is a secondary effect of NICE's main goals. As private and public sector employers become more familiar with the extent of the cybersecurity threat and the business model for addressing these threats, more jobs will be identified and created to meet these growing needs and requirements. The current administration views education and job creation as key factors for the future prosperity of this country. As such, NICE is well positioned to continue to receive the resources necessary to accomplish its mission.

NSCI: There are numerous government departments and agencies involved in NICE. How do you think we are doing in terms of clarifying the "lanes in the road" (i.e., roles and responsibilities) when it comes to cybersecurity?

MCDUFFIE: From the NICE perspective the coordination between the agencies is coming along very well. The agencies involved have been working together for a number of years now under what was CNCI-8 and now NICE. The relationships are well established and continuing to strengthen. Together we are working on the NICE Strategic Plan which will further describe the working relationship and responsibilities of the various Federal agency stakeholders. It is a different story when one speaks of overall responsibility for operational aspects of cybersecurity, which NICE is not a part of at all. Such questions should be directed to the Cyber Coordinator's office at the White House.

NSCI: If an organization has something they think can help NICE achieve its goals, how do they go about getting it considered?

MCDUFFIE: Contacting me (emcduffi@nist.gov; office number 301.975.8897) is the simplest answer to this question. We have a website already up and running http://www.nist.gov/nice which provides background information and some important links to other sites, but if you have a new idea, resources that you would like to be part of the solution, or needs that you are having trouble meeting, you should contact me. As my staff starts to stand up, eventually there will be other more specific points-of-contact that I will be able to direct individuals to but for now I'm it.

110 Royal Aberdeen ⚫ **Smithfield, VA 23430** ⚫ **ph. (757) 871-3578**

CyberPro   *National Security Cyberspace Institute*   **P a g e | 3**

NSCI: Do you have any events planned in the near future where individuals can learn more about NICE?

MCDUFFIE: As I have stated earlier, we are currently working on the NICE Strategic Plan. This Plan will become available for public comment probably in the March time frame and for 30 days. This will give the public an opportunity to learn what we are planning in some detail and to comment on those plans. In addition there will be a second annual workshop held in the greater DC area that will build on our August 2010 event. Scheduled for either later September or early October, this workshop will be the next major opportunity for the public and specific stakeholders to come together to make progress towards the NICE vision.

NSCI: Is there anything else you'd like to add?

MCDUFFIE: We are at the very beginning on a long process with large goals. Stay tuned to this space for new and exciting things to come in terms of cybersecurity education, training, and awareness. As we better define the cybersecurity workforce, it will become easier to produce the best-educated and best-trained individuals to fill these positions as that same cybersecurity workforce continues to expand. This is necessary for a competitive American cybersecurity workforce capable of meeting the challenges of the 21st century.

NSCI: Thank you very much for taking the time to visit with us.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **Page | 4**