The FDS Review

May 2021

Inside This Issue

Message from the President

Greetings team –

This past month I was happy to see more folks returning to the office here in Columbia and the continued return to normal staffing levels at our main customers. No doubt virtual meetings will be a part of our work culture for some time to come, but we are slowly moving off our screens and back into the offices. This is being facilitated by the fact that more and more people are getting their vaccines.

This month's newsletter focuses on the Cyber Operations business line, which is based in Maryland and led by Wayne Schmidt. Wayne's team has been focused on 5G work, an area of strategic importance for the DoD and the IC. Matt Wellner, a key team member of CyberOps, has provided an overview of AI and its applications. Read more on page two. In summary -- watch out for drones overhead.

Congratulations to another Matt here at FDS. Long-time employee Matt Dorty received praise from his customer at the Pentagon. Matt is a fantastic representative of the company!

What would you like to see in upcoming newsletters? Send your suggestions to FDSNEWS@feddata.com.

In closing, please don't forget to thank the moms in your life this weekend – they've earned it.

Lonny

Monthly Business Line Highlight: Cyber Operations

Cyber Operations specializes in end-to-end Computer Network Exploitation for the US Government. Our team strives to develop systems and services that deliver direct mission impacts for our customers and to provide the technical services that enable cyber operations including software development, mission management, operations planning, and operations execution. Our special project capabilities support our customers with solutions to non-traditional needs.

We are currently supporting a number of contracts, with our main focus being a large prime award on which we are tasked with creating an automated Targeting Acquisition Engine (TAE). We are exiting the prototype phases in June and moving to an operational deployment, where our team will be growing.

Another functional area of focus for our business line is new 5G opportunities. DoD is currently solicitating prototype 5G private networks for a number of bases across the US. FedData, led by Cyber Operations, has been submitting prime proposals for these opportunities as they are released. We are teamed with Dell, Intel and JMA to deliver an innovative 5G network.

Artificial Intelligence Overview

-By Matt Wellner, Cyber Operations

Artificial intelligence (AI) and machine learning (ML) have had great impacts in defense and commercial sectors over the past 20 years bringing both new capabilities and challenges with its continued advancement. Examples of these advancements lie in high visibility examples like self-driving cars and smart assistants, but, arguably the more important application of this technology is in national defense.

AI has and will continue to bring significant benefits to how the DoD conducts business. With a projected government investment of roughly $6 billion in AI for 2021, the Joint Artificial Intelligence Center (JAIC) leads the DoD in focusing on technology to improve information collection, processing, and interpretation. As the DoD continues to invest in these technologies and AI continues to mature, contract requirements for these techniques will continue to grow, adding a new dimension to how we execute on contracts.

For FedData's Cyber Operations group, AI techniques can be used to autonomously analyze networks, to find vulnerabilities, or even as a way to optimize spectrum sharing in 5G communication. As a fun way to gain experience, the Cyber Operations team is using a set of small "racing drones" equipped with a specific set of sensors to complete a series of exercises focused on sensor fusion, path planning, and machine vision. The exercises are designed to take an objective and break down that objective into increasingly more difficult steps. In our case, the steps start outside, navigating through a pre-defined flight plan and increase in difficulty until the drones can safely traverse an office-like environment without any operator assistance. The ultimate goal of our research is to develop a set of tools that can be adapted across our current and future business initiatives.

Letter of Commendation

ITS employee Matt Dorty received a letter of commendation from his Government customer. Matt is an RCDD Engineer who has been with FDS since 2015. Great job, Matt!

HEADQUARTERS, DEPARTMENT OF THE ARMY
Office of the Deputy Chief of Staff, G-3/5/7
Strategy, Plans, and Policy Directorate
400 Army Pentagon
Washington, DC 20310-0400

March 31, 2021

Dear Mr. Matt Dorty,

Thank you for your support of the G-3/5/7 and my team in the G-3/5. I am very grateful for your support and many months of effort (past and future!) to help me and my team with our Sensitive Compartmented Information Facility (SCIF) and Corridor 3 Wall Project here in the Pentagon. These two projects will improve the operational effectiveness of the G-3/5 and offer an effective way to proudly display our rich Army heritage. We have senior leadership support and it is extremely important that these projects are awarded and funded this FY. As you know the fiscal landscape changes daily and our Army Officers, DA civilians, and contractors of the G-3/5 deserve these improvements; thank you!

Again, my gratitude for your leadership and support!

Sincerely,

Bradley T. Gericke Ph.D.
Major General, U.S. Army
Director of Strategy,
Plans, and Policy

Matt -
Thank you for your great work to support us. I much appreciate your efforts.

News from Recruiting

Extended Referral Bonus Award Program

Refer your friends, associates and professional connections to join our talented and growing team!

FEDDATA is offering a referral bonus up to $10,000.

You are eligible to receive up to $10,000
in referral bonus for referrals resulting in the hiring of any of the following disciplines:

- **Forensic Analyst**
- **Intrusion Analyst**
- **Malware Reverse Engineer**
- **Network Security Engineer**

Positions require a TS/SCI with CI OR Full Scope Poly

For more details about the extended employee referral bonus program, please contact Portia Brooks, Director of Recruiting at portia.brooks@feddata.com.

VIRTUAL
CAREER FAIR

May 18, 2021
2:00 – 5:00

Our Hiring Managers will be participating in a Virtual Cleared (Polygraph Only) Hiring Event.

Tell your job-seeking friends and family to look for us there!

Contact recruiting@feddata.com for more details.

Job Title	Location
PostgreSQL/Oracle Database Administrator	Washington, DC
Senior Network Engineer	Arlington, VA
Senior Linux DevOps Engineer	Washington, DC
Senior Systems Engineer	Arlington, VA
Help Desk Technician	Laurel, MD
Discovery Analyst	Fort Meade, MD
Computer Scientist	Fort Meade, MD
Data Scientist	Annapolis Junction, MD
Software Engineer	Annapolis Junction, MD

Visit our website at https://www.feddata.com/careers/ to view a full list of ALL vacancies.

SECURITY

***Title:** Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities.*

Summary: The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) previously shared mitigations to defend against exploitation of these vulnerabilities. Knowing the tradecraft that nation-state cyber actors use along with relevant response actions will enable network defenders to focus on mitigating the vulnerabilities and techniques, enabling more comprehensive protection against adversary compromise.

https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2573391/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabili/

Protecting FedData Issued Equipment

FDS Security would like to remind you to be personally accountable for protecting the IT equipment that is issued to you, namely laptop computers. In addition to the varied Cybersecurity threats and countermeasures in place to mitigate nefarious activity, it is important to take care of the device itself, treating it as a high value item, as if it was your own.

When traveling on personal time, consider leaving your laptop at home, thus avoiding the potential for loss or theft on airplanes, in hotels and rental cars. Loss or theft of a laptop could put company or customer data at risk, will require reporting to the government and documentation in personnel security records, and of course is a monetary loss.

Please reacquaint yourself with the FedData Acceptable Use Policy, and IT Security Policy to know more on this subject. These, and all FedData policies can be found on the C2 Connection page.