# St. Johns River
## Water Management District

Michael A. Register, P.E., Executive Director

4049 Reid Street • P.O. Box 1429 • Palatka, FL 32178-1429 • 386-329-4500 • www.sjrwmd.com

DATE: February 27, 2024

TO: Interested Firms

FROM: Kendall Matott, Contracts Manager

SUBJECT: Invitation to Negotiate – 39403, Addendum 1
Cybersecurity Assessment

As a result of questions received from potential respondents, please be advised of the following changes to the subject Invitation to Negotiate:

1. As a result of the Pre-solicitation conference held on Thursday February 22, 2024, the District collected all Respondent inquires and provided clarification in the attached document: ITN 39403 - Cybersecurity Assessment Questionnaire.

2. A copy of the recorded meeting may be obtained upon request.

3. **NOTE:** Please acknowledge receipt of this Addendum in your submittal.

If you have any questions regarding this addendum, contact Kendall Matott at (386) 312-2324 or via email at kmatott@sjrwmd.com.

Attachments:

Attachment 1 – ITN 39403 Cybersecurity Assessment Questionnaire

ATTACHMENT 1 — ITN 39403 - CYBERSECURITY ASSESSMENT QUESTIONNAIRE

| | | |
|---|---|---|
| **Company Information** | | |
| | Please describe the IT team and include the number of IT departments, personnel and full-time consultants. (Please include a breakdown of roles and responsibilities for each department or individual and include the total number of individuals.) | Organizational Chart Provided (see last page). |
| | Please describe the team that is responsible for cybersecurity and compliance, including internal employees, members of the IT team and external consultants. | We don't have a dedicated Cybersecurity team. |
| | Please describe any critical IT vendors, such as MSP, MSSP, vCTO, vCISO or similar. Please include a list of these partners with their contracted roles and responsibilities. (Please include any firms for which you have contracted on-going services. If Thrive is a current vendor, please include Thrive in this list and state any contracted services.) | MSSP - TPx --> Spectrum, MDR – Arete. |
| | Is there an app development team responsible for the creation and maintenance of an app, webpage or other product utilized by clients? | Yes. |
| | How many physical offices are there? (An office is defined as a physical space with networking gear and computers, so please include home offices that will be part of this assessment.) | 10 locations, some with multiple buildings and IT Resources. The District also has a telework policy that allows employees to work remotely. |
| **IT Infrastructure** | | |
| | Please select which of the following are utilized to host email for the firm. | Office365. |
| | Does the company utilize a single identity database (such as Active Directory or Entra ID) for all sites and personnel? | Yes, the District utilizes Active Directory. |
| | Is there any infrastructure in the public cloud? | Yes. |
| | Are any of the following public cloud sites used to host servers? (Microsoft Azure/Amazon Web | Azure. |

| | | |
|---|---|---|
| | Services (AWS)/Google Cloud Platform) | |
| | Please describe the breakdown of server count per cloud hosting site and a small description of how the site is utilized (i.e. - production, development, backup, disaster recovery). | 2 - Azure – Testing. |
| | Is there any infrastructure within a colocation facility or datacenter? | No. |
| | Please describe how many servers, the type of virtualization utilized and list the number of facilities used. | Is this in reference to Q11? |
| | Is there any infrastructure in a MSP's private/community cloud? | No. |
| | Please describe how many servers and services are provided by the community cloud and a breakdown of who is responsible for each. | N/A. |
| | Please describe how many servers and any virtualization used on-premises. | The District utilizes Vmware for on-prem across four Locations |
| | Please list any SaaS platforms that are critical to the company's business or IT infrastructure. (Examples would include SSO providers or cloud-managed EDR platforms.) | The District uses multiple SaaS vendors for functions such as MFA, EDR, Password Mgmt, etc. |
| **Network** | | |
| | How many firewalls are utilized throughout the organization? (Please include the manufacturer and a breakdown of firewalls per site if possible. If they are centrally managed, please include that as well) | 11 total firewalls. |

| | | |
|---|---|---|
| | How many switches are utilized throughout the organization? (Please include the manufacturer and a breakdown of switches per site if possible. If they are centrally managed or stacked together, please include that as well.) | 51 total switches. |
| | How many wireless access points are utilized throughout the organization? (Please include the manufacturer of the wireless access points and if they are centrally managed.) | 59 total WAPs. |
| | For the penetration test noted, are you requesting an external, internal, or both types of tests? | External including lateral movement; internally if penetration is successful. Internally with guest WiFi access provided. |
| | For penetration testing purposes, can each site be accessed via a company provided VPN? | VPN connects to Palatka. From there, access is available to the other nine sites. |
| | On page 46, says assessment expected to be completed in a 9-month period. Does this mean you would like to spread out assessment over the 9 months, or that the assessment must be completed in 9 months or sooner? | Sooner is preferred; nine months is limit. |
| | What is the total number of external IPs in-scope for External Penetration Testing? | We have a full class C; 253 addresses and 10 IPs assigned to the firewalls that will likely change in the next few months when we migrate to a new service provider. |
| | What is the total number of internal network devices for the Internal Network Vulnerability Testing? | 1,349 devices as of 2/21/2024. |
| | Do you require credentialed scanning? | Not required. |
| | How are the assets separated - broadcast domains? By VPNs? By VLANS? | VLANs and BDs. Layer 3 w/ FW between WAN sites. |
| | What are the subnet sizes? | Mostly /22 and /24, some smaller. |
| | Do you utilize Microsoft Intune? | No. |
| | Do you utilize site-to-site VPNs? | Yes. |
| | Is Web Application Security Testing in-scope? If so, how many applications? | Outside of scope for this assessment. May be a recommendation coming out of the assessment. |
| | Is Wireless Penetration Testing in-scope? If so, how many sites? | Wireless penetration testing is in-scope for the Palatka and Jacksonville Service Center locations. |

| | | |
|---|---|---|
| | Is Physical Penetration Testing in-scope, if so, how many facilities will be in-scope? | Outside of scope for this assessment. |
| | Regarding Information Security (IS) Policies, how many are presently defined and implemented, and are there any that need to be developed from scratch? | One IT policy, one disciplinary policy, and seven standards/procedures. |
| | Is Social Engineering / Phishing in-scope? If so, approximately how many individuals will be targeted? | This is out of scope. |
| **Pre-Solicitaion Conference Questions** | Will the penetration testing scope also include Operational Technology? | No. |
| | Does the district intend to have 3 references listed, or 3 actual letters of reference from previous clients? | Three references listed. |
| | Does external penetration testing include social engineering and/or physical testing? | No social engineering or physical testing will be part of this engagement. |
| | I note that the estimated budget is $50,000. Would you accept proposals which are time and material? | Proposal Cost Schedule form must be completed and included in Respondent's submittal. |
| | Does the business need to be certified in the state of Florida or SAM.gov as an official women/minority owned business? | The successful Respondent must be registered to conduct business in the state of Florida. No certification with the State or SAM.gov is required. |
| | Will you accept experience from private sector clients? | Yes. |
| | For the penetration test conducted by the MSSP. How extensive was the scope? What specific aspects did they test? What are their expectations from us in terms of 'reviewing' it? | The current MSSP primarily does vulnerability scans. |
| | If questions are due 5 days before the submission date, will there be enough time to get through the questions and provide responses? Otherwise, will there be an extension to the due date past March 12th? | Every request for a written interpretation or correction must be received at least nine days prior to opening of Proposals in order to be considered. Requests may be submitted by email at kmatott@sjrwmd.com. Interpretations, corrections, and supplemental instructions will be communicated by written addenda to this solicitation posted on DemandStar and Vendor Registry to all prospective Respondents (at the respective addresses furnished for such purposes) no later than five days before the opening of Proposals. |

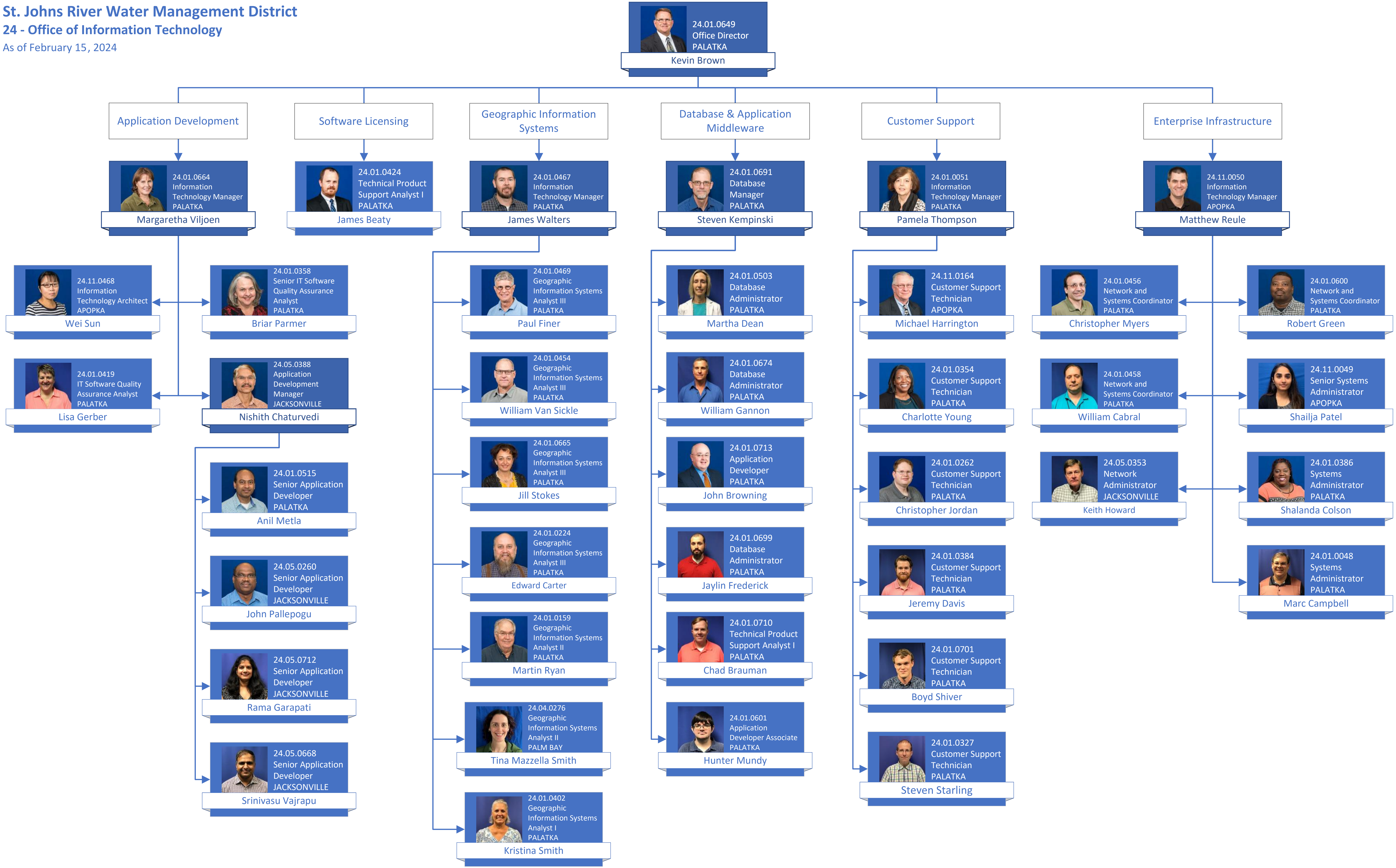
|  |  |  |
|---|---|---|
|  | Are the 10 locations on one connected network or separate networks? | All 10 are connected by an SD-WAN. |
|  | Please provide clarification on whether it is permissible for a U.S.-based entity to participate in the RFQ process on behalf of a foreign cybersecurity firm? If so, are there specific guidelines or procedures we need to adhere to in order to engage in this capacity. | All work must be done within the borders of the United States. All subconsultants must be approved by the District. The Agreement will be awarded and executed with the Successful Respondent. |
|  | How flexible is the budget for the District? | The budget is $50K and price is included in the scoring. Respondents are cautioned to not make any assumptions from the budget estimate about the total funds available for the Work. |
|  | Will the District consider any exceptions to the Terms and Conditions within the Sample agreement provided. | Respondents are encouraged to provide any exceptions with their proposal. |
|  | For various Tabs 1, 2... is the expectation to have a Tab for each section of requested information or can it all be consolidated into one proposal? | The District requests that submittals match the organizational structure outlined in Section 5. (ELECTRONIC SUBMISSION AND PREPARATION AND ORGANIZATION OF THE SUBMITTAL) of the solicitation package. |
|  | Penetration Testing, previous results would be helpful, and the number of external IP's involved (end points and IP's) | About 40 IPs. |
|  | Will a remediation scan be requested after testing and recommendations are given? | Implementation of recommendations and follow up is outside the scope of this agreement. |
|  | How many interviews do you anticipate for the NIST evaluation based on the job roles? | There are 36 IT staff. It is estimated that 15-20 interviews will be conducted. |
|  | Is the assessment going to extend into your operational technology environment? Are you looking to ingest the results into a dashboard GRC platform where raw data would be required for a seamless transition. | OT is out of scope.<br>SJRWMD does not currently use a GRC. |
|  | Do any components of the ITN or the SOW require an in-person or onsite presence?<br>Follow-up: is there a dedicated number of cyber security staff? | Not required; however, proposals must address all of the elements and identify whether they will be achieved on-site or remotely.<br>SJRWMD does not have solely dedicated positions for cyber security; this work is spread across multiple positions. |

| | | |
|---|---|---|
| | What platform is used to manage Human Resources tasks and information? | Contact SJRWMD Procurement if this is needed to prepare proposal. |
| | Is there any security monitoring in place currently? | MSSP and MDR outsourced with 24/7 SOC/NOCs. |
| | In providing a recommendation for future training, would this disqualify the vendor from bidding on future solicitations for said training. | No, the successful firm would be able to participate in future solicitations. Recommendations should not be specific to a vendor. |

# St. Johns River Water Management District

## 24 - Office of Information Technology

As of February 15, 2024



24.01.0649 Office Director PALATKA — Kevin Brown

### Application Development

- 24.01.0664 Information Technology Manager PALATKA — Margaretha Viljoen
  - 24.11.0468 Information Technology Architect APOPKA — Wei Sun
  - 24.01.0358 Senior IT Software Quality Assurance Analyst PALATKA — Briar Parmer
  - 24.01.0419 IT Software Quality Assurance Analyst PALATKA — Lisa Gerber
  - 24.05.0388 Application Development Manager JACKSONVILLE — Nishith Chaturvedi
    - 24.01.0515 Senior Application Developer PALATKA — Anil Metla
    - 24.05.0260 Senior Application Developer JACKSONVILLE — John Pallepogu
    - 24.05.0712 Senior Application Developer JACKSONVILLE — Rama Garapati
    - 24.05.0668 Senior Application Developer JACKSONVILLE — Srinivasu Vajrapu

### Software Licensing

- 24.01.0424 Technical Product Support Analyst I PALATKA — James Beaty

### Geographic Information Systems

- 24.01.0467 Information Technology Manager PALATKA — James Walters
  - 24.01.0469 Geographic Information Systems Analyst III PALATKA — Paul Finer
  - 24.01.0454 Geographic Information Systems Analyst III PALATKA — William Van Sickle
  - 24.01.0665 Geographic Information Systems Analyst III PALATKA — Jill Stokes
  - 24.01.0224 Geographic Information Systems Analyst III PALATKA — Edward Carter
  - 24.01.0159 Geographic Information Systems Analyst II PALATKA — Martin Ryan
  - 24.04.0276 Geographic Information Systems Analyst II PALM BAY — Tina Mazzella Smith
  - 24.01.0402 Geographic Information Systems Analyst I PALATKA — Kristina Smith

### Database & Application Middleware

- 24.01.0691 Database Manager PALATKA — Steven Kempinski
  - 24.01.0503 Database Administrator PALATKA — Martha Dean
  - 24.01.0674 Database Administrator PALATKA — William Gannon
  - 24.01.0713 Application Developer PALATKA — John Browning
  - 24.01.0699 Database Administrator PALATKA — Jaylin Frederick
  - 24.01.0710 Technical Product Support Analyst I PALATKA — Chad Brauman
  - 24.01.0601 Application Developer Associate PALATKA — Hunter Mundy

### Customer Support

- 24.01.0051 Information Technology Manager PALATKA — Pamela Thompson
  - 24.11.0164 Customer Support Technician APOPKA — Michael Harrington
  - 24.01.0354 Customer Support Technician PALATKA — Charlotte Young
  - 24.01.0262 Customer Support Technician PALATKA — Christopher Jordan
  - 24.01.0384 Customer Support Technician PALATKA — Jeremy Davis
  - 24.01.0701 Customer Support Technician PALATKA — Boyd Shiver
  - 24.01.0327 Customer Support Technician PALATKA — Steven Starling

### Enterprise Infrastructure

- 24.11.0050 Information Technology Manager APOPKA — Matthew Reule
  - 24.01.0456 Network and Systems Coordinator PALATKA — Christopher Myers
  - 24.01.0600 Network and Systems Coordinator PALATKA — Robert Green
  - 24.01.0458 Network and Systems Coordinator PALATKA — William Cabral
  - 24.11.0049 Senior Systems Administrator APOPKA — Shailja Patel
  - 24.05.0353 Network Administrator JACKSONVILLE — Keith Howard
  - 24.01.0386 Systems Administrator PALATKA — Shalanda Colson
  - 24.01.0048 Systems Administrator PALATKA — Marc Campbell