OAK RIDGE National Laboratory

March 2025

ORNL Updates: ETEBA

Presented by

Cassandra McGee Stuart, DBA

Mgr., Strategy and Performance, Contracts Division

U.S. DEPARTMENT OF ENERGY

ORNL IS MANAGED BY UT-BATTELLE LLC
FOR THE US DEPARTMENT OF ENERGY

Agenda

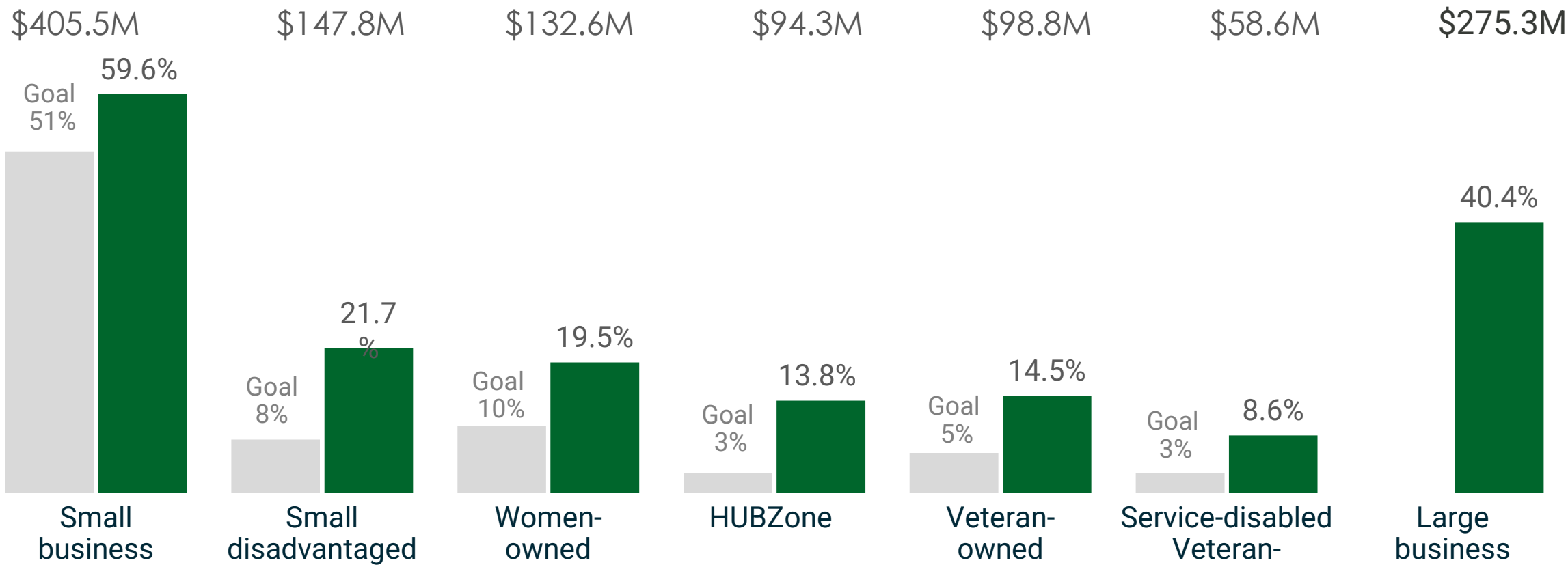
Small Business Programs – Cassandra McGee Stuart

Construction Opportunities – Kyle Young

Cybersecurity

ORNL exceeded all small business goals for FY24

Subcontract dollars placed with small business firms in FY24*

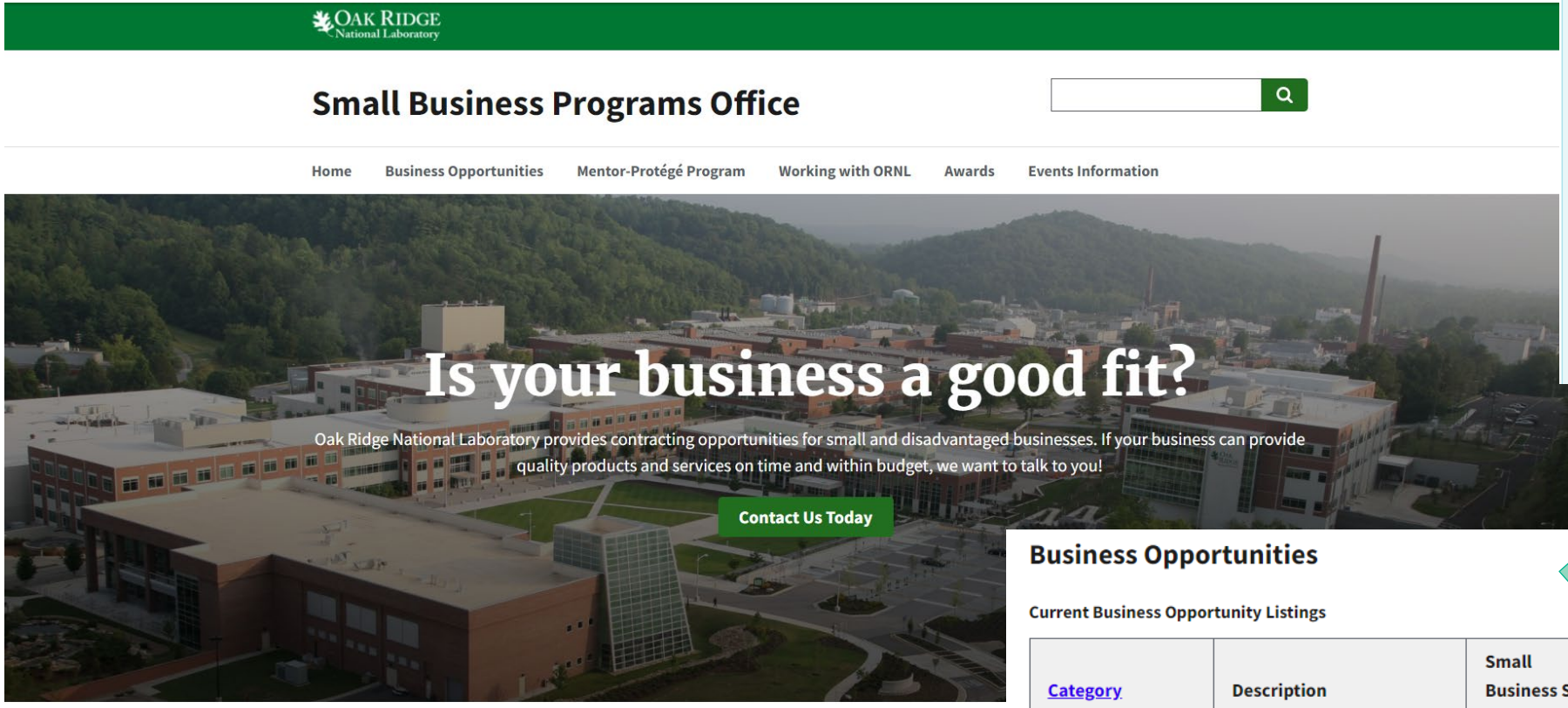


*Minus exclusions including FRGN, GOV', ING, IGT, Affiliates, Zx13, UT & P-cards.

DOE OSDBU WOSB Business Opportunity Day with ORNL and Jefferson Lab

OAK RIDGE National Laboratory

ORNL Business Opportunities



Sign up to to be notified by email when new listings are posted!

Manage your newsletter subscriptions

- Computer/IT Services
- Computer Software/Hardware
- Construction
- Fabrication and Machining Services
- Industrial and Facility Services
- Industrial Equipment
- Professional and Staffing Services
- Research & Development
- Scientific Instruments

Subscribe

Business Opportunities

Current Business Opportunity Listings

Category	Description	Small Business Set-Aside	Estimated Value	Expected Issue Date	Expected Award Date
Professional and Staffing Services	Protect Portfolio Nuclear Security Expertise (Domestic) Details	No	$15M	November 2024	February 2025
Professional and Staffing Services	Creative and Communications Services Details	No	$3.8M	November 2024	January 2025
Industrial Equipment	2nd Generation Pellet Press Details	Yes	$300,000	August/September 2024	November 2024

smallbusiness.ornl.gov

Small Business Programs Office

Cassandra McGee Stuart, Manager, Strategy & Performance
Email: mcgeecm@ornl.gov
Office: 865-576-3560

Leah Swaggerty, Small Business Program Officer
Email: swaggertylb@ornl.gov
Office: 865-341-2746

smallbusiness.ornl.gov

OAK RIDGE National Laboratory

March 2025

ORNL Construction Opportunities

Kyle Young

Construction Procurement Officer

U.S. DEPARTMENT OF ENERGY

ORNL IS MANAGED BY UT-BATTELLE LLC
FOR THE US DEPARTMENT OF ENERGY

Authorized Projects

Project	Anticipated RFP Date
Renovate Building 4500 North Library	5/2025
Replace Building 4521 Cooling Tower	5/2025
Replace Bethel Valley Campus Vehicle Bridge	7/2025
General Use High Bay Space Construction	7/2025
4000 Area Electrical Upgrade	3/2026

Upcoming Projects

Project	Anticipated RFP Date
Modernize Building 4508	10/2026
Improved 7667 Low Level Waste Site	10/2026
Improve 7603 Basement	10/2026
Multiprogram Office Building Construction	10/2027
Melton Valley Campus Support Facility	10/2027
Modernize 2000/3000 Area Utilities	10/2027
Bethel Valley Support Facility Construction	10/2028

Reoccurring Projects

- Roof Replacements
- Paving
- Lab Space Renovations
- Demolition

OAK RIDGE National Laboratory

ORNL Cyber Supply Chain Risk Management (C-SCRM)

Justin Keck

U.S. DEPARTMENT OF ENERGY

ORNL IS MANAGED BY UT-BATTELLE LLC
FOR THE US DEPARTMENT OF ENERGY

Requirement in response to DOE Order 205.1D

For applicable procurements, ORNL is required to ensure Cyber Supply Chain Risk Management (C-SCRM). This includes but is not limited to:

- *Validating vendors' assertion of maintaining minimum security controls to protect the Gov't's information systems and data*
- *Ensure vendors manage risks to their supply chain in accordance with NIST SP 800-161, C-SCRM Practices for Systems and Organizations*
- *For critical software, ensure vendors abide by the critical software requirements of OMB M-21-30*
- *And other stated requirements related to cybersecurity and supply chain risk management*

How ORNL Plans to Approach this Requirement

- Require completion of a questionnaire which will serve as the vendor's attestation of their cyber supply chain risk management practices
- The responses to this questionnaire will be evaluated and, upon confirmation of acceptable results, the procurement can proceed as planned.
- This will be similar to the Cybersecurity Maturity Model Certification (CMMC) evaluation and FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, is already in all ORNL subcontracts

C-SCRM Questionnaire

Describe how your organization does the following

1. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3. Verify and control/limit connections to and use of external information systems.
4. Control information posted or processed on publicly accessible information systems.
5. Identify information system users, processes acting on behalf of users, or devices.
6. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
7. Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
8. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
9. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

C-SCRM Questionnaire (cont.)

Describe how your organization does the following

10. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

11. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

12. Identify, report, and correct information and information system flaws in a timely manner.

13. Provide protection from malicious code at appropriate locations within organizational information systems.

14. Update malicious code protection mechanisms when new releases are available.

15. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

16. Verification of any security-related 3rd party evaluation and results of that evaluation.

ORNL is developing a guidance document for vendors to help explain each question in the questionnaire and the basis for them. This will be made available upon request from any vendor asked to complete the questionnaire.