



Welcome to the
LANL Virtual
Subcontractor
Forum

October 8, 2020

We will begin shortly



**Justin Sanchez is singing
the National Anthem**



Welcome & Opening Remarks

Presenter:

Drew Fuller, Acquisition Services Management Division Director

Agenda

- National Anthem – Justin Sanchez
- Forum Logistics – Julianna Barbee, Forum Moderator & SBDC Director - Espanola, New Mexico
- Welcome & Opening Remarks – Drew Fuller, ASM Division Director – 5 min.
- Supplier Management & Small Business Update – Chris Fresquez, ASM Supplier Management Manager
- Procurement Update – Rachel Schroeder, Transformation Management Manager – 30 min.
– Drew Fuller, ASM Division Director
- Mechanical Material Handling Policy – Jerome Trujillo, OSH-ISH Safety Team Leader – 15 min.
– Tom Courtney, OSH-ISH
- Cybersecurity – Elythia McAnarney, New Mexico PTAC Advisor 30 min.

Agenda - Continued

- Cyber Awareness Brief – Becky Rutherford & William Clark NIE-ESS – 5 min.
- Scorpius Project Opportunities – Mike Cisneros, ASM Scorpius Team Leader – 15 min.
- Supply Chain Management Center (SCMC) and Strategic Sourcing Opportunities – Maureen Armijo, ASM Center of Excellence Team Leader – 20 min.
- Multiple Award Task Order Contract (MATOC) Update – Susan Stein, ASM Capital Projects – 15 min.
- Organizational Changes – Capital Projects – Susan Stein & Brad Westergren – 10 min.
- Closing Remarks – Yvonne Gonzales-Small Business Advocate



Supplier Management and Small Business Update

Presenter:

Chris Fresquez, Supplier Management Manager

Updates

- FY20 Small Business Statistics
- FY21 Small Business Goals
- eSRS action items
- SAM Update – Unique Entity Identifier
- Small Business Resource Engagement
- Outreach events
- Business Opportunities
- Recognition

Small Business Statistics

Small Business Categories	FY20 Goals	FY20 Accomplishments
Small Business	61.70%	65.3%
Small Disadvantaged Business	27.50%	16.8%
Woman Owned Small Business	19.50%	16.3%
HUBZone Small Business	4.95%	5.9%
Veteran Owned Small Business	8.50%	5.3%
Service Disabled Veteran Owned Small Business	4.70%	2.0%

Small Business Goals

Small Business Categories	FY21 Goals
Small Business	63.70%
Small Disadvantaged Business	27.50%
Woman Owned Small Business	19.50%
HUBZone Small Business	4.95%
Veteran Owned Small Business	8.50%
Service Disabled Veteran Owned Small Business	4.70%

eSRS - Action Items & Deadlines

Primarily for subcontracts exceeding \$700K, or \$1.5M construction

- If Subcontracting Plan is in effect, then...
 - eSRS ISR - Data entries due for period ending September 30 have been extended as follows:
 - **ISR reports due November 30**
 - **SSR reports due December 30**
 - Reporting is for the 6 month period (April 1, 2020 through September 30, 2020),

If you require assistance, please contact the LANL Small Business Program at **“business.lanl.gov”**

SAM Update – Unique Entity Identifier

- The U.S. Government is moving to a new Government-owned Unique Entity Identifier (UEI) which will ultimately become the primary key to identify entities throughout SAM, other IAE systems, and downstream Government systems.
- The DUNS® will be phased out as the primary key to identify every entity record within SAM.
- This was originally scheduled to take place in December 2020, it has been postponed.

Small Business Resource Engagement, Training, and Supplier Development

- Small Business Administration (SBA)
- Procurement Technical Advisory Centers (PTAC)
- Small Business Development Centers (SBDC)
- Service Core of Retired Executives (SCORE)
- Regional Development Corporation (RDC)
- Chambers of Commerce
- Department of Energy – Office of Small & Disadvantaged Business Utilization (OSDBU)

SBA FIRST WEDNESDAY VIRTUAL LEARNING SERIES

FY 2021 SCHEDULE

1:00 to 2:00 PM Central Time

FY 2021	Date	Topic
1	October 7, 2020	8(a) Program
2	November 4, 2020	SBIR/STTR Program
3	December 2, 2020	Surety Bonds
4	January 6, 2021	Size and Affiliation
5	February 3, 2021	Consolidation/Bundling
6	March 3, 2021	Women Owned Small Business (WOSB) Program
7	April 7, 2021	All Small Mentor Protégé Program (ASMPP)
8	May 5, 2021	Certificate Of Competency (COC)
9	June 2, 2021	Regulatory Updates
10	July 7, 2021	Subcontracting Program
11	August 4, 2021	TBD

The program schedule is for information only and is subject to change.

SBA - SCORE (Service Core of Retired Executives)

[X] The linked image cannot be displayed. The file may have been moved, renamed, or deleted. V...

[X] The linked image cannot be displayed...

Local Events (ABQ/RR)

- Through 12/31: On Demand Webinar - Economic Injury Disaster Loan
- Through 12/31: On Demand Webinar - PPP Loan Forgiveness Application Requirements
- 10/1: First Session
- 10/13: Ask the Expert: One Hour of Q&A on Business Start Ups
- 10/20: Ask the Expert: One Hour of Q&A on Marketing
- 10/21: First Session
- 10/21: Expert Tips to Buying and Selling a Business
- 10/27: Ask the Expert: One Hour of Q&A on Business Funding
-

Webinars (live)

- 10/8: How to Explain Your Products and Services with Infographics
- 10/14: Women-Owned Startups in Rural America - Learn About Useful Tools & Resources
- 10/15: Where's The Money Now? Position Your business for the Future of Small Business Lending
- 10/20: Increase Your Sales with Online Reviews
- 10/22: Financing Tips to Make Your E-Commerce Business Thrive During Peak Season
- 10/29: Funding Options for Hispanic Owned Businesses in the "Missing Middle" Gap
- 11/3: Year-End Tax Planning for Your Business
- 11/5: Re-Strategize Your Business Planning to Prevail the Pandemic

- Request a Mentor NOW!
- All SCORE Recorded Webinars
- All SCORE Courses on Demand
- SCORE Business Learning Center

[X] The linked imag...

Local Events (ABQ/RR/Los Lunas)

- 10/8: Webinar - Developing Social Media Marketing Strategies (Session 3)
- 10/7: Basic Steps to Starting a Business in New Mexico 2020
- 10/15-16: #QuickBooks Pro for your Small Business (2-day Workshop)
- 10/21: Basic Steps to Starting a Business in New Mexico 2020
- 10/28: #QuickBooks Online
- 11/4: Basic Bookkeeping for the Small Business Owner
- 11/4: Basic Steps to Starting a Business in New Mexico 2020

[X] The linked image cannot be...

Local Events (ABQ/Los Lunas)

- Watch this space for PTAC events coming in November!

[X] The linked image cannot b...

Local Events (ABQ/RR)

- 10/8: Revisit Your Personal Budget: Managing the Impacts of COVID-19
- 10/13: WESST Virtual Small Business Series: How to get More 5-Star Reviews on Google
- 10/19: The Journey to Authentic Leadership in COVID Times
- 10/21: Women Who Own It Speaker Series
- 10/22: WESST Virtual Small Business Series: Principles of Social Media Marketing
- 10/28: WESST Lunch 'n Learn: Understanding Merchant Services for Small Business

[X] The linked image cannot be...

Local Events (ABQ)

- 10/6: Lunch & Learn: Managing Uncertainty - Go From Fearful to Focused in 3 Steps
- 10/7: Community Connects Call
- 10/13: Lunch & Learn: Time Mastery for the Present and Future
- 10/14: Community Connects Call
- 10/20: Lunch & Learn: Presentation Skills 101
- 10/21: October Virtual Meeting - More Clients, Less Marketing
- 10/21: Community Connects Call
- 10/27: Lunch & Learn: The Power of Authority
- 10/28: Community Connects Call
- 11/4: Community Connects Call

[X] The linked L...

Local Events (ABQ)

- 11/5: Power in Partnership: Executive Assistant Workshop

[X] The linked image canno...

Local Events (ABQ)

- Entrepreneurship Bootcamp for Veterans
- Business Fundamentals
- Boots to Business/Reboot
- Online Courses

[X] The li...

Local Events (ABQ)

- 10/20: New Mexico Prosperity Virtual Summit
- 10/27: Small Business Resiliency Virtual Workshop
- Online Courses to Start and Run Your Business

Special Thanks to SCORE Albuquerque's 2020 Sponsors

SBDC

Small Business Development Center at Northern New Mexico College

America's Business Experts Assisting America's Job Creators

SBDC Your Local, National, Global Business Resource

Helping Entrepreneurs Start New Businesses, Grow Existing Businesses and Stay in Business.

Are you looking to grow or start a business? Is your business profitable? Would you like to increase revenues? Do you have a dream and want to make it a reality?

SBDC's help small businesses create jobs

America's SBDC (Small Business Development Centers) network of certified business experts is the leading national business resource offering no-cost consulting and low-cost training that inspire small businesses and entrepreneurs to grow, create jobs and build the economy.

SBDC'S help all small businesses, all stages, all types and all industries

SBDC's provide assistance and training in Business Development, Business Plans, Marketing Plans, Financial Plans, Social Media, Website Development, Technology, eCommerce, Access to Capital, Tax Planning, Legal Issues, Government Contracting, International Trade, Managing a Business, Growing a Business, Start-up Assistance, Access to local, national and global partners and much more!

Española, New Mexico SBDC awarded Job Creator and SBDC Center of the Year

Española SBDC continues to be recognized nationally for its dedication to business success, economic impact, measurable performances, sustainable outcomes and innovative opportunities.

STAFF

Julianna Barbee, Director jbarbee@nnmc.edu

Rita Sandoval, Business Advisor rtamm@nnmc.edu

PTAC Events

Space is limited! Register SOON!

Contract Ready Series Parts I - V

Dates & Times: 2020

- Part I: Thursday, September 17th - 9:00 am - 11:00 am
- Part II: Thursday, September 17th - 1:00 pm - 3:00 pm
- Part III: Wednesday, September 23rd - 9:00 am - 11:00 am
- Part IV: Wednesday, September 23rd - 1:00 pm - 3:00 pm
- Part V: Tuesday, September 29th - 9:00 am - 12:00 pm

 The linked image cannot be displayed. The file may have been moved, renamed, or deleted. V...

Cost:

No Charge

Location: Webinar

- Zoom webinar information will be sent out the day before each event.
- Email ptac@sfcc.edu if you would like to confirm your registration.

You MUST register for each Part individually (links available below)

Part I: Understanding Solicitations – <https://nmsbdc.ecenterdirect.com/events/12733>
A comprehensive look at the components of a solicitation

- Learn a process for solicitation review
- Learning how to decipher evaluation criteria to make a smart "bid" or "no bid" decision.

Part II: Proposal Writing – <https://nmsbdc.ecenterdirect.com/events/12734>

Topics Include:

- Deciphering proposal instructions
- The method and process for Requests for Proposals (RFPs)
- Types of proposal content required
- Common Proposal Mistakes
- Understanding the big picture of procurement processes

Part III: Labor Law Compliance – <https://nmsbdc.ecenterdirect.com/events/12735>

Topics Include:

- An overview of US Labor Laws
- Understanding compliance to Federal Contracting specific laws: Service Contract Act, David Bacon, Walsh Healy, and various Executive Orders

Part IV: Estimating & Pricing – <https://nmsbdc.ecenterdirect.com/events/12736>

Topics Include:

- Learn why having a budget (for start-ups) or good financial statements (for existing firms) is the key to good pricing
- Element by element, learn how to "build" a bill rate
- Be able to build a basic cost proposal
- Get familiar with common pricing problems and learn how to avoid them

Part V: Contract Administration – <https://nmsbdc.ecenterdirect.com/events/12737>

Topic includes

- Learn about the structure of the Federal Acquisition Regulations – so you can find what you need quickly.
- Learn about key elements of contract compliance and best practices for ensuring compliance

Understand some common contract administration problems and how to avoid them.
ptac@sfcc.edu or 505-224-5965 for more information

The New Mexico Procurement Technical Assistance Center (NMPTAC) is funded in part through a cooperative agreement with the Defense Logistics Agency. The NMPTAC is also funded by the State of New Mexico.

Office of Small and Disadvantaged Business Utilization – (OSDBU)

- Partner at future LANL Subcontractor Forums
- The Office of Small and Disadvantaged Business Utilization (OSDBU) implements and executes Sections 8 and 15 of the Small [Business Act \(SBAAct\)](#).
- Per Section 15, small businesses must receive a fair proportion of the total purchases and contracts for property and services for the federal government.
- Success in this objective is measured by the Department's demonstrated efforts to:
 - exceed statutory prime, sub and socio-economic small business goals;
 - provide education on the management and operations business model;
 - improve best practices such as the Mentor-Protégé Program;
 - furnish information on financial assistance opportunities;
 - train small businesses through outreach events and training opportunities;
 - ensure compliance with Federal Acquisition Regulations and other applicable small business laws and regulations;
 - issue new small business policies;
 - and update existing small business policies at the Department.

LANL Specific Topics

- Safety
- Security
- Quality
- Environmental
- Lessons Learned
- REA development
- Tracking DCO related costs
- Project Scheduling
- Project Submittals
- LANL Engineering Standards
- Business Development
- Responding to an RFP
- Terms and Conditions

Upcoming Outreach Events

- LANL Virtual Subcontractor Forums
 - Monthly
- Third Thursday of the month (dates subject to change)
 - November 12, 2020
 - December 17, 2020
 - January 21, 2021
 - February 18, 2021
 - March 18, 2021

LANL Subcontractor Forum Distribution List

- The Small Business Program Office is updating the FY2021 Subcontractor Forum Listing and need your help to ensure we have current contact information.
- A registration link will be sent out today (10/8/2020) after the forum.
- We encourage you to complete this registration because we will be using as an invitation listing for future forums.
- Registration link will close on October 22, 2020.
- Contact the Small Business Program Office at business@lanl.gov for questions.

Business Opportunities

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

ABOUT | MISSION | BUSINESS | NEWSROOM | PUBLICATIONS

SEARCH SITE

SCIENCE & INNOVATION | COLLABORATION | CAREERS | COMMUNITY | ENVIRONMENT

Business > **Planned and Open Procurement Opportunities**

Planned and Open Procurement Opportunities

We seek to do business with qualified companies offering value and high-quality products and services.

Current business opportunities at Los Alamos

SCAM ALERT: Los Alamos National Laboratory has recently been advised from other DOE national laboratories of fraudulent attempts to procure goods from legitimate laboratory suppliers. Find more information on the [SCAM Alert letter \(pdf\)](#).

- **Short-Term Business Opportunities** are normally competitive business opportunities greater than \$250K that will be posted for seven calendar days.
- **Long-Term Business Opportunities** are normally competitive business opportunities greater than \$250K that have a projected date greater than the seven calendar days.

> [Guidance on process](#)

Short-Term Business Opportunities

Click the **ID#** below to view the associated Business Opportunity Document.

Short Term Opportunities

ID #	Title of Opportunity	Est. Dollar Value	Competition Type
019	Radioactive Laundry and Respirator Services	TBD	Open Procurement
180	NGA-1 Plumbing Supplier	TBD	TBD
171	Paving Projects	TBD	TBD
175	ECSD-ASD Project	TBD	TBD
228	Civil Design Package for Temporary Trailer Site	TBD	Small Business Set Aside
242	Paving MTOA	TBD	TBD
315	IBC Test and Inspection MTOA	TBD	TBD

Long-Term Business Opportunities

Long Term opportunities listed below are provided as an informational resource only. Due to the nature of these business opportunities, they are subject to change or cancellation due to scope, mission, or funding requirements. For updated information on these opportunities please look for updates that will be posted on this website as they become available.

Click the **ID#** below to view the associated Business Opportunity Document.

Long Term Opportunities

ID #	Title of Opportunity	Est. Dollar Value	Competition Type
224	Mud Rooms Renovation	TBD	TBD
275	Restore functionality to Train Doors	TBD	TBD
319	RFI Metals IDIQ	TBD	TBD
320	RFI NGA-1 Subcontractors	TBD	TBD

Construction Indefinite Delivery-Indefinite Quantity (IDIQ) Multiple Award Task Order Contract (MATOC)

- IDIQ MATOC
- MATOC Cover Letter
- J-1 Exhibit F
- J-2 Exhibit C
- J-3 Exhibit H
- Attachment L-1

Links to forecasted opportunities: DOE, other agencies and facilities

- DOE acquisition forecast¹⁷
- Sandia National Laboratories' business opportunities
- Quantal 200 Mercury Treatment RFP
- Beta.SAM.gov contract opportunities

BUSINESS

[Business Home](#)

SUPPLIER OUTREACH

[Procurement Transformation](#)
[Supplier Diversity](#)
[Supply Chain Principles](#)

SUPPLIER RESOURCES

[Becoming a Supplier](#)

Calendar

[COVID-19 Business Resources](#)

[Invoicing and Payment](#)

[Links](#)

[Planned and Open Procurement Opportunities](#)

[Supplier Forms](#)

[Terms and Conditions](#)

CONTACT US

[Business Contact List](#)

General Inquiries
 (505) 667-4419
business@lanl.gov



Contacts | Media | Calendar
 Inside | Terms of Use, Privacy | Site Feedback
 Managed by Triad National Security, LLC for the U.S. Dept. of Energy's NNSA |
 © Copyright Triad National Security, LLC. All Rights Reserved.



© JNS



Request for Interest

Posting Date: 12/17/2019

Posting Close Date: TBD

Estimated Period of Performance: TBD

Competition Type: TBD

Contact Email: chrisam@lanl.gov; business@lanl.gov

Title: Restore Functionality to Train Doors

Description of Product or Service Required

We are looking to locate a vendor to perform work involved to restore functionality to some hydraulic powered shielding doors. This work will be performed in a Radiological Buffer Area and a High Contamination area. We have the design done and parts specified.

Description:

We are an older facility and produce isotopes for medical, industrial and R&D applications. We have 13 hotcells arranged in a "U" shape. There is a shielding door on each end of the "U". These doors were previously operated with hydraulic cylinders from the house hydraulics, which have been removed long ago. The doors are currently being propped up and not operational. There is an existing cylinder and limit switches on each door which would be replaced with new. Each door would have its own reservoir and pump. The new hydraulics would be connected to the existing hard lines then to the cylinders. All of this would be controlled with existing control panels at the cells on each end of the "U". Cells 1 and 12.

In general, there will need to be hydraulic cylinders, reservoirs w/ pumps, and limit switches installed. Programming would then be added to control the doors. We will also need to have a couple of 120v circuits installed (install conduit, pull wires) where the external pumps will be."

- Current forecasted bid opportunities are subject to change or cancellation due to scope, mission, or funding requirements.
- Some procurements are reserved for small businesses. Note the competition type on the forecast matrix to determine if a procurement has been set aside or is open to fair and reasonable competition.
- LANL reserves the right to change the competition type from Competitive to Set-Aside prior to the release of the Request for Quotation (RFQ).
- If this is a Request for Expression of Interest and capability information is requested with your response, be advised that LANL will not issue your organization a Request for Quotation unless you submit clear and convincing information that your organization has the necessary relevant experience and can fulfill the requirements of the statement of work. If you do not adequately address the required information, and the LANL Buyer does not have information indicating otherwise, the presumption will be that your organization is not a viable competitor. In any case, the LANL Buyer is the final arbiter on who receives an RFQ.

SBP 003 2/25/2015

1

Current and Upcoming Business Opportunities

- Gloveboxes – Randy Martin
- SCORPIUS Project - Michael Cisneros
- MSP & Staff Augmentation Project – Ed Ybarra
- Subcontracting partnerships with MATOC subcontractors

– Visit us at “www.lanl.gov/business”

LANL Recognition

- DOE 2019 Facility Management Contractor Small Business Achievement of the Year:
 - Triad National Security, LLC
- DOE 2019 Laboratory Director of the Year:
 - Dr. Thomas Mason, Director, Triad National Security, LLC

Local Recognition

- TruNet Computer Technology, Espanola, NM
 - SBA Family owned Business of the year
 - Jeffery Atencio, President
- Black Mesa Winery, LLC, Velarde NM
 - SBA Home Based Small Business of the Year
 - Jerry and Lynda Burd, Owners
- Performance Maintenance Incorporated
 - DOE Hubzone Subcontractor of the Year
 - Eric Quintana, President





Questions



Procurement Transformation at LANL

Moving to an all-new Digital Procurement System
October 8 2020

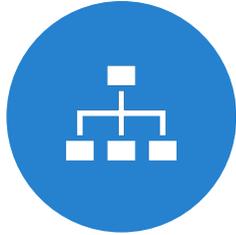
Presenters

Drew Fuller, Acquisition Services Management Division Director &
Rachel Schroeder, Transformation Management Manager

LANL HAS EMBARKED ON A MAJOR PROCUREMENT TRANSFORMATION



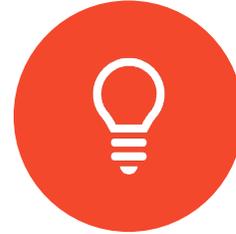
**ATTRACT AND
QUALIFY NEW
SUPPLIERS**



**BUILD AND
ENHANCE
RELATIONSHIPS
WITH OUR
SUPPLIERS**



**DEVELOP AND
MENTOR OUR
SUPPLIERS**



**MODERNIZE AND
STREAMLINE OUR
PROCUREMENT
ACTIVITIES AND
TOOLS**

You — the supplier — are an important part of the Laboratory's success. We are excited to invite you to join us on this journey!

WHERE ARE WE HEADED?

Procurement at LANL is going digital — with new systems that will enable our suppliers to interact with LANL digitally in real-time.



Who does this apply to?

- All suppliers

We will need all suppliers to move to our new systems as they are rolled out



What's changing?

- New, digital systems
- Streamlined, transparent processes

New systems include:

- ✓ SAP Ariba 
- ✓ SAP Fieldglass 
- ✓ CertFocus  by Vertical

Our new integrated solutions will completely automate the end-to-end, source-to-pay procurement processes

WHAT ARE THE BENEFITS?



Your improved future experience

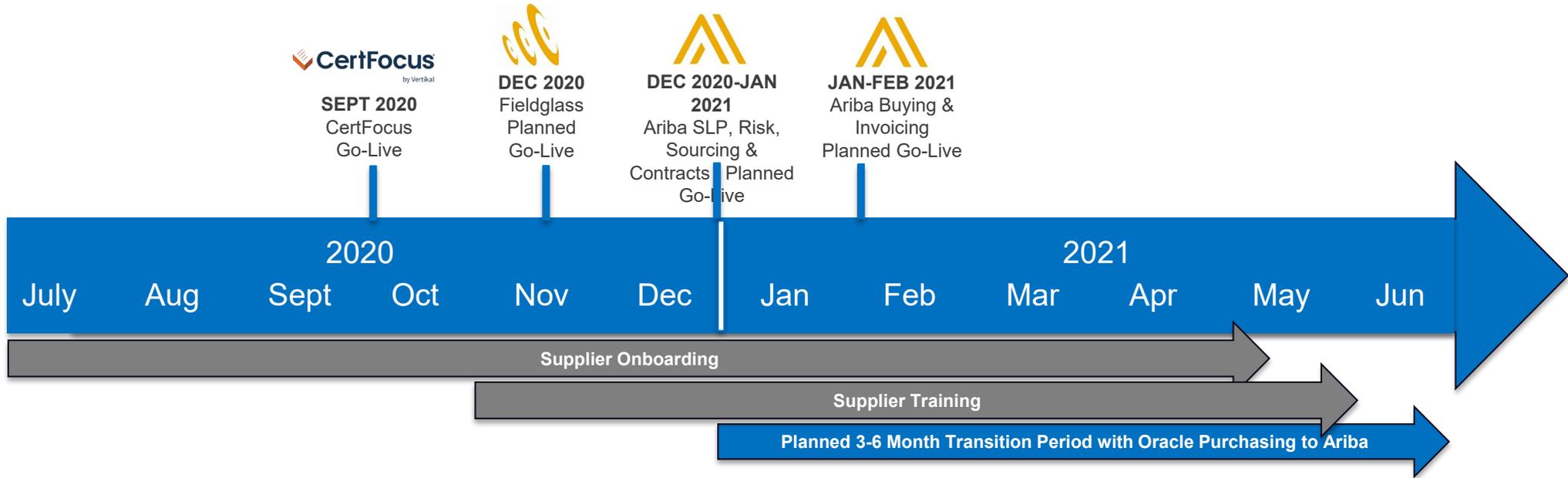
Our goal is to make it **easier** to do business with LANL

- ✓ Completely **electronic transactions** such as purchase orders and invoices
- ✓ **Simplified** interactions with LANL with more efficient communication
- ✓ **Greater transparency** of business interaction status with LANL 24/7/365
- ✓ Increased **efficiency** and **accuracy** of PO and invoicing processes
- ✓ More **control** over order processing
- ✓ **Faster** payment
- ✓ **Save time and money** by eliminating paper and manual processing
- ✓ Keep track of documents with a **searchable** archive

The new procurement systems and processes will have substantial positive impacts and supplier benefits

TIMELINE AND ROADMAP

We are planning to roll out the new systems in a phased approach as shown in the timeline below. We need all suppliers to be ready for the Go-Live dates.

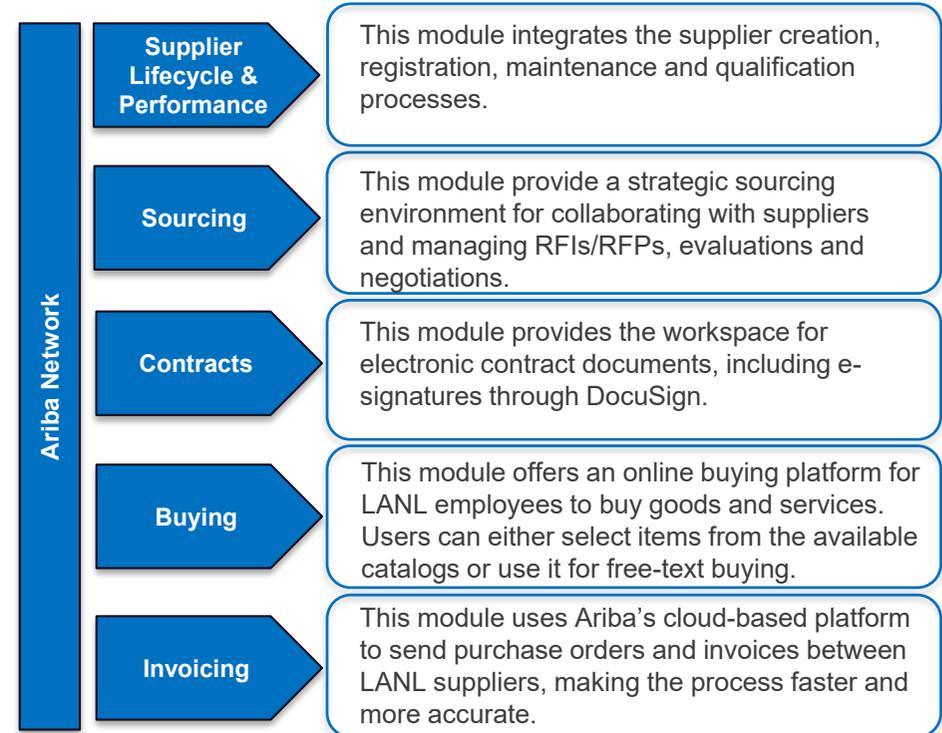


We are committed to supporting you during this transition and will communicate with you about actions required and timing

INTRODUCING SAP ARIBA

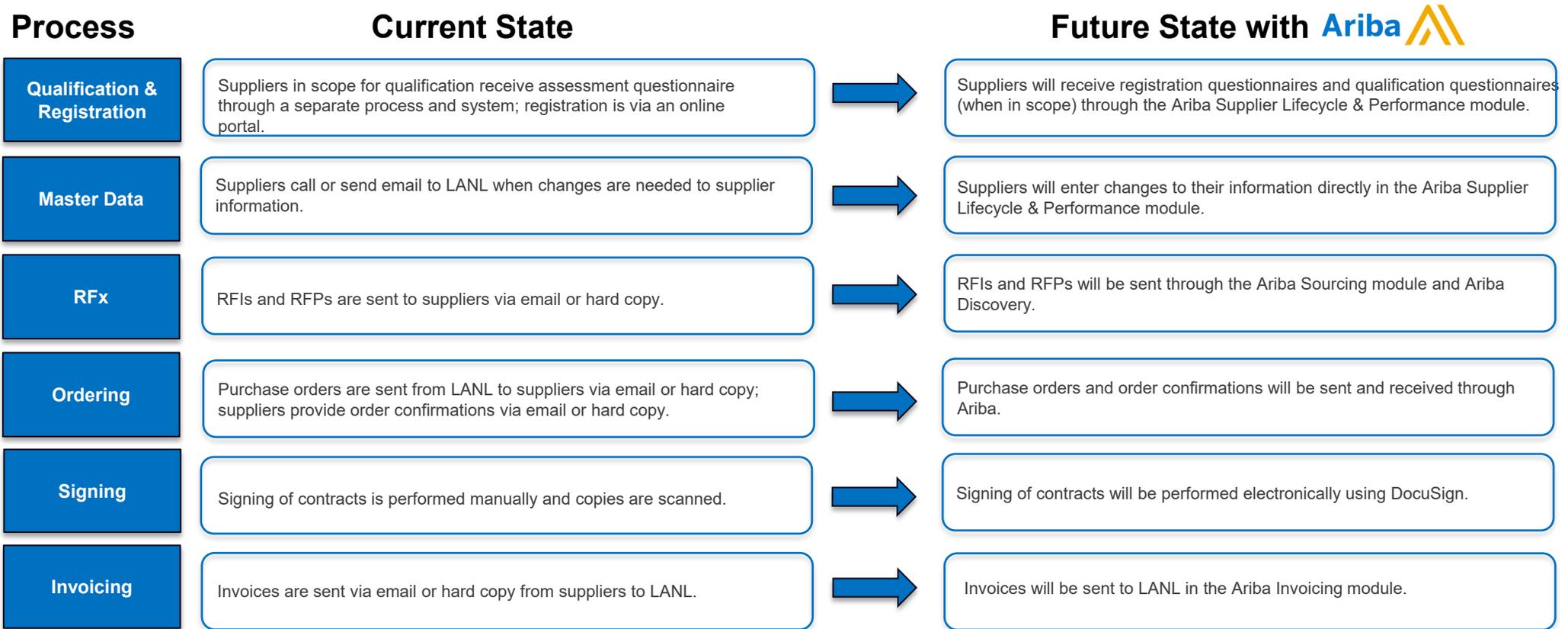
- Ariba is a cloud-based business-to-business collaboration platform where millions of companies interact.
- The implementation of SAP Ariba will include the five underlying Ariba modules, the Ariba Network and Ariba Discovery.
- The implementation offers one integrated portal for LANL to collaborate effectively with suppliers when we buy, invoice, select, negotiate agreements and manage information and relationships.
- After Go-Live, buying and purchase requisitions will be performed in Ariba. Future solicitations and awards conducted via Ariba.

We are implementing five underlying Ariba modules



We are enabling world-class procurement through one portal for supplier collaboration – all in a simple, compliant and efficient way

WHAT ARE THE KEY PROCESS CHANGES?



The integrated modules and automated workflows in Ariba will provide significant benefits to suppliers

SAP Ariba Account Types

There are two SAP Ariba account types available for suppliers. Both account types can be used to transact with LANL. The Standard account is always free of charge, while the Enterprise account is generally subject to fees.

Standard Account

- **Free-of-charge** access to all SAP Ariba modules needed to transact with LANL.
- Access is always initiated via an **interactive email** attached to the order.
- Collaborate on **all basic document types**: orders, order confirmations and invoices.
- Receive **Invoice Status Notifications** in real-time and view scheduled payment dates.
- Access can be provided to **multiple users** in the supplier organization.
- **Mobile** enabled and it is free.

Enterprise Account

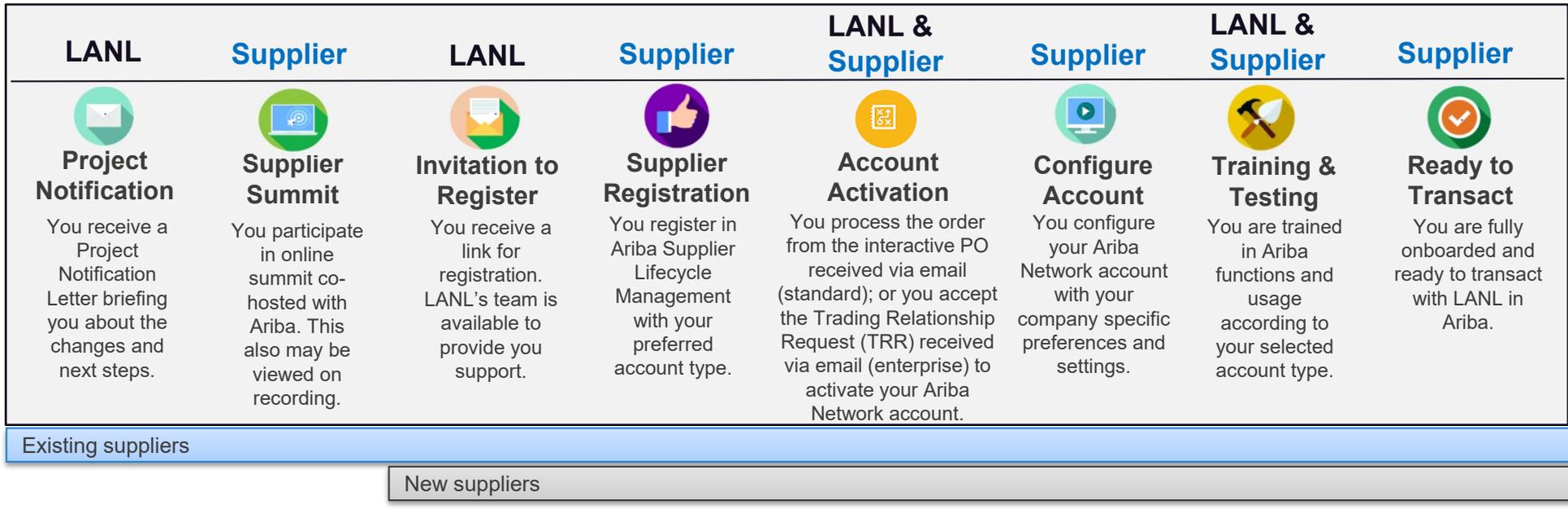
- Supplier funded subscription is **subject to fees**.
- **Online dashboard** to get and manage orders and invoices all on the Ariba Network.
- Enables **back-end integration** with a Supplier ERP system.
- Provides the ability for suppliers to **manage own catalogs**.
- **Invoices are archived** online for the life of the account.
- Dedicated live-chat, phone and email **support included** from SAP Ariba.
- Enhanced **reporting** capabilities.

As a supplier, you can choose the account type that best suits your needs

HOW TO GET STARTED IN ARIBA

Onboarding of **existing LANL suppliers** will be done in phases. LANL will ensure all suppliers receive the information and support needed during the transition. Once Ariba is deployed, all **new LANL suppliers** will be instructed to sign up directly through Ariba.

The supplier onboarding process



We are committed to helping suppliers get started in Ariba

INTRODUCING SAP FIELDGLASS

Overview

- **SAP Fieldglass** will automate the contract worker purchasing process, from the creation of the job requisition, interview and screening process, applicant selection, expense and time keeping, invoicing and reporting. The system is web-based and can be accessed from any computer that has internet access.

Supplier Benefits

- **Single point-of-contact** for suppliers for any contract worker need
- **A standardized and responsive process** for acquisition and deployment of contingent labor resources
- **Improved** financial control and reporting
- **A flexible solution** that is scalable with ever-changing business requirements

What's changing?

- Implementing a LANL-owned instance of the Fieldglass Contingent Worker Vendor Management system
- All contingent labor transactions (procuring, time-keeping and expense reporting) will go through the new LANL instance of Fieldglass
- New Managed Service Provider (MSP), AgileOne, has been hired to manage the program



- Replaces the current version of the COMPA instance of Fieldglass Contingent Worker Vendor Management system
- Currently, only contingent labor through COMPA utilizes the Fieldglass system. Other contingent labor suppliers operate through manual processes outside of Fieldglass
- Replaces current model

We are standardizing the process and streamlining the time it takes to find and procure qualified contingent labor

INTRODUCING CERTFOCUS

Overview

LANL has engaged Vertikal to monitor and track insurance compliance and the collection process of insurance certificates using the CertFocus system

Benefits

- Specific insurance requirements are posted on CertFocus for easy access.
- Insurance certificates can be submitted directly by your insurance broker via web upload, email or fax to Vertikal for entry into the CertFocus system, a friendly and time- and cost-saving alternative to mailing, receiving, monitoring and filing paper insurance certificates.
- The CertFocus system is available 24 hours a day, seven days a week and requires no special software installations; all you need is a computer and internet access.
- No log-in or password is needed.
- LANL will be notified of receipt of your insurance certificate. The insurance certificate will be rejected if non-compliant with the contract requirements. CertFocus will provide you with non-compliant notes to help you and your broker resolve this matter.



LEARN MORE

Visit LANL's website to learn more about our Procurement Transformation initiative:

lanl.gov/business

Los Alamos National Laboratory
Delivering science and technology to protect our nation and promote world stability

About Mission Business Newsroom Publications

search site

SCIENCE & INNOVATION COLLABORATION CAREERS COMMUNITY ENVIRONMENT

Business

Business

We seek to do business with qualified companies offering value and high-quality products and services.



Do business with us

BUSINESS

[Business Home](#)

SUPPLIER OUTREACH

[Procurement Transformation](#)

[Supplier Diversity](#)

[Supply Chain Principles](#)

SUPPLIER RESOURCES

Visit LANL's Ariba Supplier Information Portal to find Ariba training, resources and guides:

support.ariba.com/item/view/186986

Los Alamos NATIONAL LABORATORY EST. 1943

Welcome to the Supplier Information Portal

SAP Ariba

Welcome to the LANL Supplier Information Portal. This portal provides information for all suppliers that are conducting business with LANL. For our suppliers, this means that the traditional way of interacting with us, is changing fundamentally. On this site you will find information regarding the transformation and hopefully answers to many of your questions.

What information are you looking for?

	Project Notification Letter Regarding the Ariba Network		Introduction to Ariba Network Enterprise Account Summit with Q&A Standard Account (coming soon)		Ariba Network Account Configuration Training
--	--	--	--	--	--

	Live Demos Useful Links		How to use the Help Center and Other Support Options		Fees
--	--	--	--	--	----------------------

	Integration & Catalog Catalog & Integrations processes for transacting via the Ariba Network. Catalog Portal Link Integration Portal (coming soon)		LANL FAQs		Quick Reference Training Clips Learn how to set up your Ariba account
--	---	--	---------------------------	--	--



For questions or technical support, please contact the LANL Supplier Management team at

aribasuppliers@lanl.gov



LANL CONTACTS

LANL Procurement Transformation

- Rachel Schroeder, Procurement Transformation Manager

LANL Small Business Program

- Yvonne Gonzales, Small Business Program

LANL Catalog Enablement

- Cole McGee, Catalog Management

LANL Supplier Management Desk

- Susan Sprake, Supplier Enablement and Qualification
- Ashley Dominguez, Supplier Enablement and Qualification
- Trish Alley, Supplier Enablement and Qualification
- Richard Martinez, Supplier Enablement and Qualification

aribasuppliers@lanl.gov

LANL Supplier Performance Management

- Dan Brown, Supplier Performance Management
- Dereck Willis, Supplier Performance Management



Visit LANL's Website for Contact Information: lanl.gov/business



Questions



Mechanical Material Handling Policy Subcontractor Forum

Presenter:
Jerome Trujillo & Tom Courtney, OSH-ISH

Mechanical Material Handling Procedure P101-40

- Scope – Work activities that involve moving materials by various types of equipment that provide a mechanical advantage
- Why
 - Several material handling events at LANL and at other DOE sites
 - Identified gap in guidance and policy
- Policy Development
 - Culmination of 1.5 years in development
 - Engagement with other DOE sites
 - Internal LANL engagement with multiple stakeholders



Mechanical Material Handling - PROCESS OVERVIEW

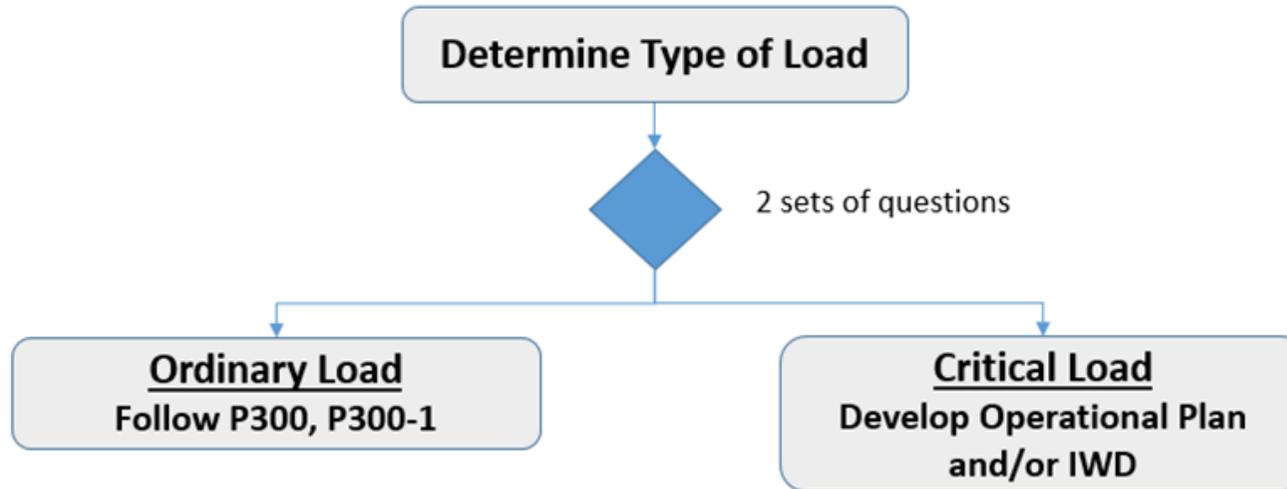


Exhibit F63 - Mechanical Material Handling Summary

- Replaces Jack and Roll Operations, RN101-25-01
- Subcontractors determine if MMH task is for Ordinary or Critical Load
 - ✓ Determination reviewed and approved by STR and LANL MMH Coordinator
 - ✓ If Critical Load, then sub works with STR and LANL MMH Coordinator on Critical Load Operations Plan; Attachment F63-1 is guide and template
 - ✓ Plan supplements IWD → IWD update process

F63 – Mechanical Material Handling

F63.2

- SUBCONTRACTOR is required to evaluate mechanical material handling (MMH) work activities to make a load determination of Ordinary Load or Critical Load.
- *SUBCONTRACTOR shall provide CONTRACTOR STR with proposed load determination and STR, with assistance from CONTRACTOR MMH Coordinator as needed, must concur before MMH task planning continues.*
- After SUBCONTRACTOR and CONTRACTOR agreement on the determination of Ordinary Load or Critical Load, SUBCONTRACTOR is required to complete the requirements associated with the selected load type.

F63 – Subcontractor Actions

- Answering the screening question in F63, the Subcontractor provides the STR with the proposed determination of Ordinary Load or Critical Load for the MMH activity. Subcontractor can communicate this determination via an email that explains how the MMH task is to be completed.
- Prior to conducting MMH Critical Load tasks, subcontractor will develop a Critical Load Operations Plan with input from the STR and applicable LANL MMH Coordinator, as appropriate. Subcontractor will submit the plan to the STR. The plan is incorporated into, or use a supplement to, the task IWD. As such, this is considered an update to the IWD and subcontractor will follow the IWD review and approval process.
- Attachment F63-1, *Critical Load Operational Plan Instructions and Sample Template* can be used by subcontractors when developing the plan.

F63-1 Critical Load Operational Plan

- <https://int.lanl.gov/safety/exhibit-f/downloads/Attachment-F63-1.pdf>

Mechanical Material Handling – LANL CONTACTS

- Contacts
 - Program Lead: Jerome Trujillo, OSH-ISH
 - Subject Matter Experts:
 - Jerome Trujillo, OSH-ISH
 - Tom Courtney, OSH-ISH
 - Phil Romero, OSH-ISH



Questions



CYBERSECURITY/

LEARN CONNECT WIN !

The New Mexico Procurement Technical Assistance Center (NMPTAC) is funded in part through a cooperative agreement with the Defense Logistics Agency.
The NMPTAC is also funded by the State of New Mexico.

Overview

- ▶ Regulatory Requirements
- ▶ Controlled Unclassified Information
- ▶ NIST Frame work
- ▶ Meeting FAR 52.204–21 Requirements

What is Cybersecurity?

- ▶ The activity or process, ability or capability, or state, whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Federal Information System

- ▶ An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
- ▶ Samples of executive agency : Department of Defense and Department of Homeland Security.
- ▶ —Federal Information security Management Act (40 U.S.C., Sec. 11331)

Nonfederal Organizations

- ▶ An entity that owns, operates, or maintains a nonfederal information system.
- ▶ Some Examples
 - Federal contractors, and subcontractors.
 - State, local and tribal governments.
 - Colleges and universities.
- ▶ – NIST Special Publication 800-171

Cyber Security Compliance Requirements

- ▶ **FAR 52.204-21**
- ▶ Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
- ▶ 2014 and 2016 Implementation
- ▶ No Grace Period for Compliance
- ▶ 15 Controls
- ▶ Considered Minimum Compliance Criteria
- ▶ Controlled Unclassified Information (CUI)
- ▶ **NIST SP 800-171**
- ▶ **Special Publication: Protecting Unclassified Information in Nonfederal Information Systems and Organizations**
- ▶ Sets Industry Standard Practice
- ▶ 110 Controls
 - Physical Site Controls
 - Computer System Controls
 - Process Security Controls

<https://www.acquisition.gov/content/regulations>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>

Do not Comply

- ▶ Contractors who do not comply with these requirements are subject to Termination for Default.
- ▶ 31 U.S. Code § 3729. False claims
 - Knowingly present or cause to be presented to the United States a false or fraudulent claim for payment or approval (31 U.S.C. § 3729(a)(1)(A));
 - Knowingly make, use, or cause to be made or used a false record or statement to get a false or fraudulent claim paid or approved (31 U.S.C. § 3729(a)(1)(B))

Protecting Controlled Unclassified Information

- ▶ The principle force behind the government's contractor cybersecurity requirements is protecting against the loss of critical intellectual property and sensitive information.
- ▶ Billions of dollars worth of Research and Development data has been stolen by various individuals or nation states allowing them to leap ahead of the US without significant costs
- ▶ Critical defense or privacy information is being stolen and sold

The CUI Registry

- ▶ Online Repository
- ▶ Identifies approved CUI categories
- ▶ Includes procedures for CUI items
- ▶ www.archives.gov/cui/registry/category-list.html

CUI Categories Index Grouping

- ▶ Critical Infrastructure
- ▶ Defense
- ▶ Export Control
- ▶ Financial
- ▶ Immigration
- ▶ Intelligence
- ▶ International Agreements
- ▶ Law Enforcement
- ▶ Legal
- ▶ Natural and Cultural Resources
- ▶ North Atlantic Treaty Organizational (NATO)
- ▶ Nuclear
- ▶ Patent
- ▶ Privacy
- ▶ Procurement and Acquisition
- ▶ Proprietary Business Information
- ▶ Provisional
- ▶ Statistical
- ▶ Tax
- ▶ Transportation

CUI Category – Example

Organizational Index_Grouping	CUI Categories
Financial	<ul style="list-style-type: none">• Bank Secrecy• Budget• Comptroller General• Electronic Funds Transfer• Federal Housing Finance Non-Public Information• General Financial Information• International Financial Institutions• Mergers• Net Worth• Retirement

CUI Category: Electronic Funds Transfer

Category Description:	Relating to the computer-based systems used to perform financial transactions electronically.
Category Marking:	XFER
Banner Format and Marking Notes;	<p>Banner Format: CUI//Category Marking//Limited Dissemination Control</p> <p>Marking Notes:</p> <ul style="list-style-type: none">•Category Marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control•Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control•Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI.•Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control•Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control•Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control•Reference 32 CFR 202.20, CUI Marking Handbook, Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines.

National Institute of Standards and Technology (NIST)

- ▶ NIST is a Non regulatory agency
- ▶ NIST serves as the U.S. National Measurement Institute
- ▶ NIST provides neutral technical expertise, guidance and reference materials

Cybersecurity Framework

- ▶ NIST tasked to provide guidance
 - Protecting Controlled Unclassified Information
- ▶ Task Completed June 2015
- ▶ NIST Special Publication 800-171

NIST Cybersecurity Framework

- ▶ The NIST Cybersecurity Framework, created thru collaboration between govt. & private sector, uses common Language to address and manage cybersecurity risk in cost-effective way based on business needs

- ▶ FRAMEWORK CORE:

- Identifies
- Protect
- Detect
- Respond
- Recover



Security Requirements

▶ NIST 800–171 Security Families

▶ AC – Access Control (3.1)	22
▶ AT – Awareness & Training (3.2)	3
▶ AU – Audit & Accountability (3.3)	9
▶ CM – Configuration Management (3.4)	9
▶ IA – Identification & Authentication (3.5)	11
▶ IR – Incident Response (3.6)	3
▶ MA – Maintenance (3.7)	6
▶ MP – Media Protection (3.8)	9
▶ PS – Personnel Security (3.9)	2
▶ PE – Physical Protection (3.10)	6
▶ RA – Risk Assessment (3.11)	3
▶ CA – Security Assessment (3.12)	4
▶ SC – System & Communications Protection (3.13)	16
▶ SI – System & Information Integrity (3.14)	<u>7</u>
▶ TOTAL REQUIREMENTS:	<i>110</i>

3-Step Process to Complying with Cybersecurity Requirements



- ▶ **STEP 1: Develop System Security Plan (SSP) describing**
 - The system boundary;
 - The operational environment;
 - How the security requirements are implemented; and
 - The relationships with or connections to other systems

- ▶ **STEP 2: Conduct Assessment, Produce Security Assessment Report**
 - Conducted against security requirements in NIST SP 800-171

- ▶ **STEP 3: Produce a Plan of Action with Milestones (POAM)**
 - Should describe how any unimplemented security requirements will be met and how any planned improvements will be implemented
 - Should include detailed milestones used to measure progress

What Security Measures are “Adequate”

- ▶ **No Systems are completely secure.**
- ▶ **But can we really define “adequate retrospectively?”**
 - Your security was not adequate if you did not employ industry and sector appropriate measures.
 - Your security was not adequate if you did not have a plan to secure your systems
 - Your security was not adequate if you did not perform a risk assessment.
- ▶ **If you did all these and still were breached, then the answer is less clear.**
- ▶ **NIST SP 800–171 describes good practices that must be followed. If they are not followed, then your security measures are definitely not “Adequate”.**

Securing the Supply Chain

- ▶ The Cybersecurity requirements do not simply apply to the prime contractor
- ▶ Cybersecurity is a mandatory flow-down requirement to lower tier contractors and subcontractors at all levels
- ▶ This is even true of the Basic FAR: FAR 52.204-21 requirements in Commercial Contracts!
- ▶ The intent is to secure the entire supply chain at all levels.

Prime Contractor Responsibilities

- ▶ Fundamental requirement to manage subcontractors (see Far 42.202(e)(2))
- ▶ Remember, the only actual parties to a Government contract are the Government and the prime contractor
- ▶ Understand what constitutes CDI under the clause
- ▶ – CDI includes unclassified CTI or other information contained in NARAs CUI Registry
- ▶ Maintain an open, written dialogue with the CO to determine the type of data at play
- ▶ Ensure that the clause is appropriately included in subcontracts

Prime Contract Responsibilities (Cont.)

- ▶ Conduct proper due diligence on all proposed subcontractors
- ▶ Understand the consequences of noncompliance
 - – Breach
 - – Termination
 - – Past Performance Issues
 - – Potential FCA allegations

NIST 800-171A

- ▶ NIST 800-171A will be used to assess the compliance of CUI security requirements.
- ▶ This will be used by Contracting Officers and Prime contractors.
- ▶ There are a total of 320 assessment objectives

NIST 800-171 Compliance

‣ NIST 800-171 Security Families	R1	Objectives	A
‣ AC – Access Control (3.1)	22	48	70
‣ AT – Awareness & Training (3.2)	3	6	9
‣ AU – Audit & Accountability (3.3)	9	20	29
‣ CM – Configuration Management (3.4)	9	35	44
‣ IA – Identification & Authentication (3.5)	11	14	25
‣ IR – Incident Response (3.6)	3	11	14
‣ MA – Maintenance (3.7)	6	4	10
‣ MP – Media Protection (3.8)	9	6	15
‣ PS – Personnel Security (3.9)	2	2	4
‣ PE – Physical Protection (3.10)	6	10	16
‣ RA – Risk Assessment (3.11)	3	6	9
‣ CA – Security Assessment (3.12)	4	10	14
‣ SC – System & Communications Protection (3.13)	16	25	41
‣ SI – System & Information Integrity (3.14)	<u>7</u>	<u>13</u>	<u>20</u>
‣ TOTAL REQUIREMENTS:	110	210	320

NIST/FAR Requirements

NIST 800-171 Security Families	R1	Objectives	A	FAR
AC – Access Control (3.1)	22	48	70	4
AT – Awareness & Training (3.2)	3	6	9	
AU – Audit & Accountability (3.3)	9	20	29	
CM – Configuration Management (3.4)	9	35	44	
IA – Identification & Authentication (3.5)	11	14	25	2
IR – Incident Response (3.6)	3	11	14	
MA – Maintenance (3.7)	6	4	10	
MP – Media Protection (3.8)	9	6	15	1
PS – Personnel Security (3.9)	2	2	4	
PE – Physical Protection (3.10)	6	10	16	4
RA – Risk Assessment (3.11)	3	6	9	
CA – Security Assessment (3.12)	4	10	14	
SC – System & Communications Protection (3.13)	16	25	41	2
SI – System & Information Integrity (3.14)	7	13	20	4
}TOTAL REQUIREMENTS:	110	210	320	17

FAR: Basic Safeguarding of Covered Contractor Information Systems

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	800-171 Family
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	Access Control
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	Access Control
(iii) Verify and control/limit connections to and use of external information systems.	3.1.20	Access Control
(iv) Control information posted or processed on publicly accessible information systems.	3.1.22	Access Control
(v) Identify information system users, processes acting on behalf of users, or devices.	3.5.1	Identification and Authentication
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	Identification and Authentication
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3	Media Protection

FAR: Basic Safeguarding of Covered Contractor Information Systems (Cont)

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	800-171 Family
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1	Physical Protection
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	3.10.3 3.10.4 3.10.5	Physical Protection
(x) 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.	3.13.1	System and Communication Protection
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	System and Communication Protection
(xii) Identify, report, and correct information and information system flaws in a timely manner.	3.14.1	System and Information Integrity
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.2	System and Information Integrity
(xiv) Update malicious code protection mechanisms when new releases are available.	3.14.4	System and Information Integrity
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5	System and Information Integrity

Access Control (AC)

FAR 52.204-21 b.1.i

- ▶ Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
 - Control who can use company computers and who can log on to the company computers.
 - Set up your system so that unauthorized users and devices cannot get on the company network.
 - NIST SP 800-171 3.1.1

Access Control (AC)

FAR 52.204-21 b.1.ii

- ▶ Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
 - Make sure to limit users/employees to only the systems, roles, or applications they are permitted to use and that are needed for their job.

- NIST SP 800-171 3.1.2

Access Control (AC)

FAR 52.204-21 b.1.iii

- ▶ Verify and control/limit connections to and use of external information systems.
 - Make sure to control and manage connections between your company network and outside networks, such as public internet or a network that does not belong to your company.
 - Be aware of applications that can be run by outside systems.
 - Control and limit personal devices like laptops, tablets, and phones from accessing the company networks and information.

Access Control (AC)

FAR 52.204-21 b.1.iv

- ▶ Control information posted or processed on publicly accessible information systems.
 - Do not allow sensitive information, including FCI, to become public.
 - It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website.
 - Limit and control information that is posted on your company's website(s) that can be accessed by the public.
 - NIST SP 800-171 3.1.22

Identification and Authentication (IDA)

FAR 52.204-21 b.1.v

- ▶ Identify information system users, processes acting on behalf of users, or devices.
 - Authentication helps you to know who is using or viewing your system.
 - Make sure to assign individual, unique identifiers, like user names, to all employees/users who access company systems.
 - Confirm the identities of users, process, or devices before allowing them access to the company's information system—usually done through passwords.
 - NIST SP 800-171 3.5.1

Identification and Authentication (IDA)

FAR 52.204-21 b.1.vi

- ▶ Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
 - Before you let a person or a device have access to your system, you need to verify that user or device is who or what it claims to be.
 - This verification is called authentication.
 - The most common way to verify identity is using a username and a hard-to-guess password.
 - NIST SP 800-171 3.5.2

Media Protection (MP)

FAR 52.204-21 b.1.vii

- ▶ Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
 - In this case, “media” can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones.
 - It is important to see what information is on these types of media.

Media Protection (MP)

FAR 52.204-21 b.1.vii (cont.)

- If there is Federal contract information (FCI) – information you or your company got doing work for the Federal government that is not shared publicly–you or someone in your company should do one of two things before throwing the media away:
 - Clean or purge the information, if you want to reuse the device, or
 - Shred or destroy the device so it cannot be read.

NIST SP 800-171 3.8.3

Physical Protection (PP)

FAR 52.204-21 b.1.viii

- ▶ Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
 - Think about what parts of your physical space (office, plant, factory, etc.) what equipment, including the network, need to be protected from physical contact.
 - For those parts of your company where you want only specific employees to have physical access to, monitor or limit who is able to enter those spaces with badges, key cards, etc.
 - NIST SP 800-171 3.10.1

Physical Protection (PP)

FAR 52.204-21 Partial b.1.ix

- ▶ Escort visitors and monitor visitor activity.
 - Do not allow visitors, even those people you know well, to walk around your facility without an escort.
 - Make sure that all non-employees wear special visitor badges and/or are escorted by an employee at all times while on your property.

- NIST SP 800-171 3.10.3

Physical Protection (PP)

FAR 52.204-21 Partial b.1.ix

- ▶ Maintain audit logs of physical access.
 - Make sure you have a record of who is accessing both your facility (office, plant, factory, etc.) and your equipment.
 - You can do this in writing by having employees and visitors sign in and sign out as they enter and leave your physical space, and be keeping a record of who is coming and going from the facility.

- NIST SP 800-171 3.10.4

Physical Protection (PP)

FAR 52.204-21 Partial b.1.ix

- ▶ Control and manage physical access devices.
 - Controlling physical access devices like locks, badging, key cards, etc. Is just as important as monitoring and limiting who is able to physically access certain equipment.
 - Locks, badges, and key cards are only strong protection if you know who has them and what access they allow.

- NIST SP 800-171 3.10.5

System and Communication Protection (SCP) FAR 52.204-21 b.1.x

- ▶ 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.
 - Just as your office or plant has fences and locks for protection from the outside, and uses badges and keycards to keep non-employees out, your company's IT network or system has boundaries that must be protected.
 - Many companies use a web proxy and a firewall.
 - NIST SP 800-171 3.13.1

System and Communication Protection (SCP)

FAR 52.204-21 b.1.xi

- ▶ Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
 - Separate the publicly accessible systems from the internal systems that need to be protected.
 - Do not place the internal systems on the same network as the publicly accessible systems.

- NIST SP 800-171 3.13.5

System and Informational Integrity (SII)

FAR 52.204-21 b.1.xii

- ▶ Identify, report, and correct information and information system flaws in a timely manner.
 - Be aware of problems in the software and computer equipment your company uses.
 - Consider purchasing support from your hardware and software vendors/suppliers, getting patches, and signing up for IT newsletters with updates about common problems or weaknesses in software.
 - Install security updates promptly.
 - NIST SP 800-171 3.14.1

System and Informational Integrity (SII)

FAR 52.204-21 b.1.xiii

- ▶ Provide protection from malicious code at appropriate locations within organizational information systems.
 - You can protect your company's valuable IT system by stopping malicious code at designated locations in your system.
 - Malicious code is program code that purposefully creates an unauthorized function or process that will have a negative impact on the confidentiality, integrity, or availability of an information system.
 - A designated location may be your network device or your computer.
 - NIST SP 800-171 3.14.2

System and Informational Integrity (SII)

FAR 52.204-21 b.1.xiv

- ▶ Update malicious code protection mechanisms when new releases are available.
 - You can protect your company's valuable IT systems by staying up to date on new security releases that stop malicious code and monitoring the system regularly.
 - Malicious code is program code that is always changing, so it is important to always have up-to-date protections, such as anti-malware tools.
 - NIST SP 800-171 3.14.4

System and Informational Integrity (SII)

FAR 52.204-21 b.1.xv

- ▶ Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
 - Companies should use anti-malware software to scan and identify viruses in their computer systems, and have a plan for how often scans are conducted.
 - Real-time scans will look at the system whenever new files are downloaded, opened, and saved.
 - Periodic scans check previously saved files against updated malware information.
 - NIST SP 800-171-3.14.5

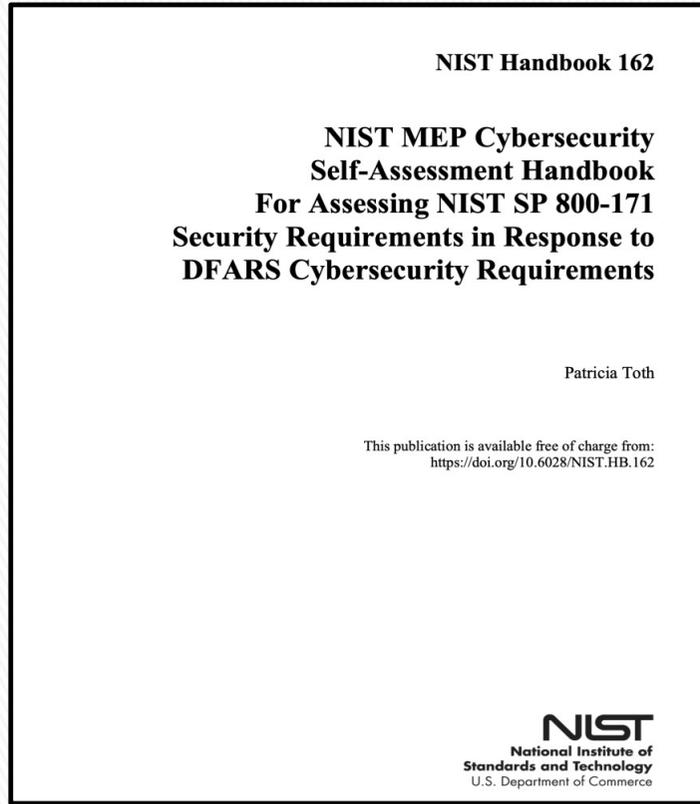
Items to consider

- ▶ Self- Assessment of devices
- ▶ Policies regarding use of company equipment
- ▶ Cybersecurity Insurance
- ▶ Computer files backup
- ▶ Train Employees
 - Employees are your first line of defense
 - They need to feel and understand this
 - Need to know what to look for
 - Who can they go to with questions

Perform a Self-Assessment

- ▶ Use NIST Handbook 162 to perform a Self-Assessment of your company.
 - Not everything in this handbook will apply to every business situation.

<https://csrc.nist.gov/publications/detail/sp/800-162/final>



CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C001 Establish system access requirements	P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight	P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules. • NIST SP 800-171 3.1.9	
		P1006 Limit use of portable storage devices on external systems. • NIST SP 800-171 3.1.21	
C002 Control internal system access	P1002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 3.1.2	P1007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 3.1.5 • UK NCSC Cyber Essentials	P1017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf

Summary

- ▶ FAR Clause 52.204-21 should be in place already
- ▶ NIST Special Publication 800-171 defines security requirements for CUI
- ▶ Federal Acquisition Regulation (FAR) are currently being updated to include SP 800-171

Links of Resources Available

Resources Available

- ▶ FAR Clause 52.204-21
 - <https://www.acquisition.gov/content/regulations>
- ▶ NIST SP 800-171
 - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>
- ▶ CUI Registry
 - <https://www.archives.gov/cui/registry/category-list>

Resources Available

- ▶ Cybersecurity Self-Assessment Handbook (NIST Handbook 162)
 - <https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf>
- ▶ Cybersecurity Template
 - <https://gtpac.org/cybersecurity-training-video/>
- ▶ U.S. Department of Energy (DOE O 205.1C)
 - <https://www.directives.doe.gov/directives-documents/200-series/0205.1-BOrder-c/@@images/file>

Resources Available

- ▶ System Administration, Networking, and Security (SANS)
 - <https://www.sans.org/account/loginsso>
- ▶ Stay Safe Online
 - <https://staysafeonline.org/>
- ▶ Department of Homeland Security
 - <https://www.us-cert.gov/resources/assessments>
- ▶ Federal Trade Commission
 - <https://www.ftc.gov/tips-advice/business-center/small-businesses>

Resources

- ▶ Project Spectrum
 - <https://projectspectrum.io/#!/>
 - Project Spectrum is an initiative supported by the [Department of Defense Office of Small Business Programs.](#)

References

- ▶ NIST Presentation 10/18/2017
 - David Stieren, Division Chief, Programs and Partnerships
- ▶ Georgia Institute of Technology
 - The Georgia Institute of Technology, commonly referred to as Georgia Tech, is a public research university in Atlanta, Georgia, in the United States.
- ▶ Webinars
 - Cyber Collaboration Center
 - Resilience
 - NICE (National Initiative for Cybersecurity Education)
 - USC University of Southern California

Thank you for joining us today

For More Information Contact:

Elythia McAnarney
PTAC Advisor

Elythia.mcanarney@sfcc.edu

505-224-5964

www.nmptac.org



Cyber Awareness Brief

Presenter:

Becky Rutherford & Bill Clark, NIE-ESS

What is BEC (Business Email Compromise)?

- **BEC is when a threat actor uses social engineering to compromise the victim's email account. This is usually done via a phishing email.**
- **Once the account is compromised, the attacker will find ways to maintain persistence in the account. They might set up a very similar email for victims to reply to, but send messages from the legit email account.**
- **The victim's email account can then be weaponized and used to send fake invoices, or requests to update billing information, in order to redirect funds to the criminal's account.**
- **If a vendor's account is compromised, it can have a negative impact both on the vendor and their customers.**

BEC in the News

- **Xoom corporation suffered a BEC attack where spoofed emails were sent to the company's finance department. These resulted in over \$30 million being wired overseas to fraudulent accounts.**
- **Ubiquiti Networks suffered a BEC attack involving employee and executive impersonation via emails to their finance department. This resulted in over \$46 million being wired overseas to fraudulent accounts.**
- **Mattel suffered a spear phishing attack targeted to an executive authorized to approve large money transfers. The attackers had conducted thorough research on the company and knew exactly what to say and whom to talk to. This attack resulted in \$3 million being wired overseas to fraudulent accounts.**
- **This is a small sampling. In 2019 alone, BEC cost businesses over \$1.7 billion. The average cost of a BEC attack in 2020 is about \$80,000.**

Types of BEC

- **CEO Fraud:** Attackers pose as the CEO or executive of a company and email an individual in finance, or possibly an admin, requesting funds to be transferred to an account controlled by the attacker, or gift cards.
- **Account Compromise:** An employee's email account is hacked and is used to request payments from vendors. Payments are then sent to fraudulent bank accounts owned by the attacker.
- **False Invoice Scheme:** The scammer acts as if they are the supplier and request fund transfers to fraudulent accounts.
- **Attorney Impersonation:** This is when an attacker impersonates a lawyer or legal representative.
- **Data Theft:** These types of attacks target HR employees in an attempt to obtain personal or sensitive information about individuals within the company. This data can then be leveraged for future attacks such as CEO Fraud, or used for identity theft.

How to prevent BEC

- Use two-factor authentication to verify any change to account information or wire instructions.
- Continuously educate your end users with a cyber awareness program.
- Check the full email address on any message and be alert to hyperlinks that may contain misspellings of the actual domain name.
- Do not supply login credentials or personal information in response to a text or email.
- Regularly monitor financial accounts.
- Consider implementing DMARC/SPF/DKIM to prevent email spoofing of your domain. These are ways to authenticate your mail server, and prove to others that you are not being spoofed. Your IT department can help you set this up.
- Immediately contact LANL if you suspect you have been a victim of email compromise. You can email csirt@lanl.gov

BEC Examples

From Bruce Wayne <info@1egit-c0mpany.com> ☆ Reply Reply All Forward More

Subject **Payment** 4/4/2017, 12:52 AM

To finance@legit-company.com ☆

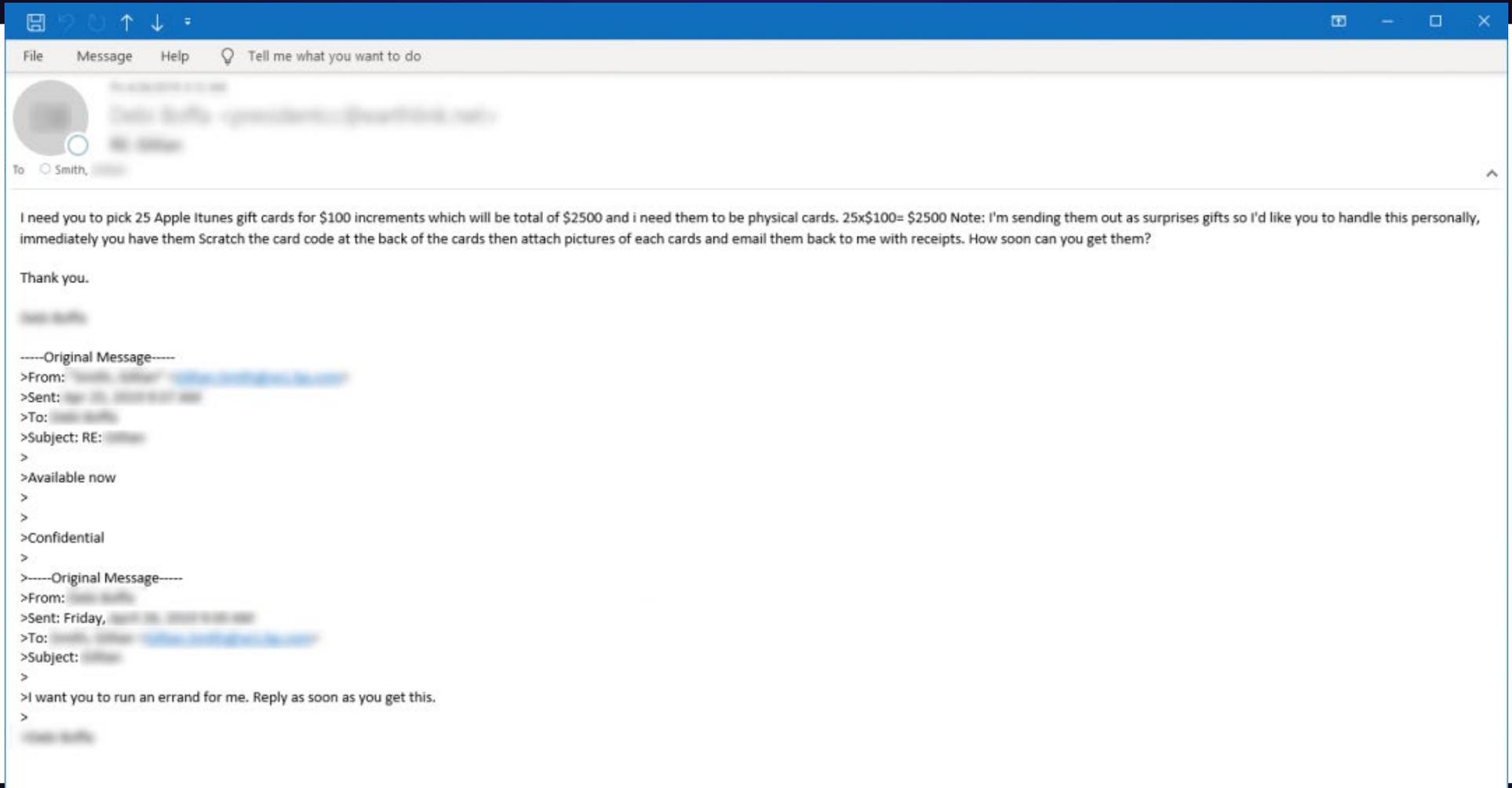
Morning,

Are you at your desk right now?Kindly get back to me so i can send you today wire instruction which i want you to execute..

Kind regards

Bruce Wayne

BEC Examples



The screenshot shows an email client interface with a blue header bar containing navigation icons and a search bar. The message header shows a profile picture of 'John Smith' and the recipient 'Smith, John'. The main body of the email contains a request for 25 Apple iTunes gift cards, a thank you note, and two quoted email messages. The first quoted message is a header with fields for From, Sent, To, and Subject. The second quoted message is a header with fields for From, Sent, To, and Subject, followed by the text 'I want you to run an errand for me. Reply as soon as you get this.'

File Message Help Tell me what you want to do

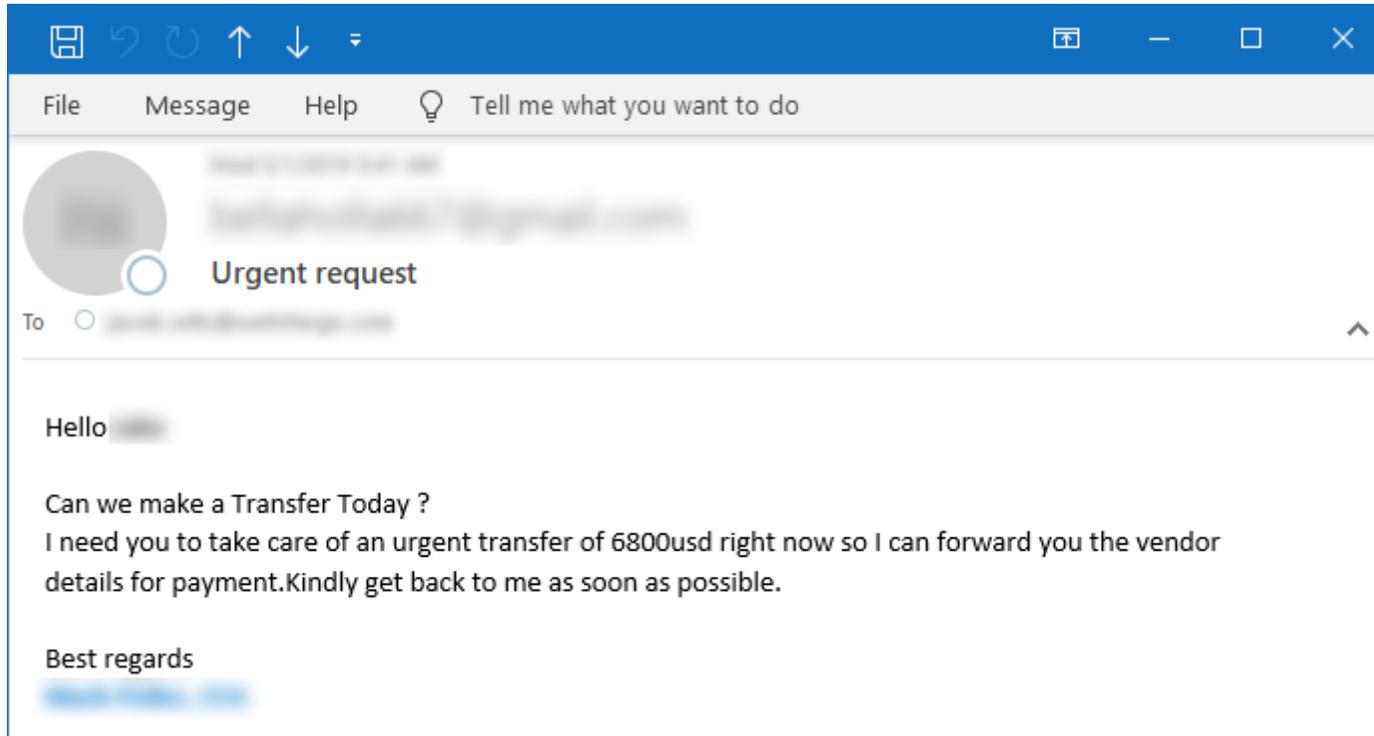
John Smith
To: Smith, John

I need you to pick 25 Apple iTunes gift cards for \$100 increments which will be total of \$2500 and i need them to be physical cards. $25 \times \$100 = \2500 Note: I'm sending them out as surprises gifts so I'd like you to handle this personally, immediately you have them Scratch the card code at the back of the cards then attach pictures of each cards and email them back to me with receipts. How soon can you get them?

Thank you.

-----Original Message-----
>From: John Smith
>Sent:
>To: John Smith
>Subject: RE:
>
>Available now
>
>
>Confidential
>
>-----Original Message-----
>From: John Smith
>Sent: Friday,
>To: John Smith
>Subject:
>
>I want you to run an errand for me. Reply as soon as you get this.
>
>

BEC Examples



References

- <https://resources.infosecinstitute.com/5-real-world-examples-business-email-compromise/>
- <https://www.proofpoint.com/us/threat-reference/business-email-compromise>
- [https://www.darkreading.com/fbi-business-email-compromise-cost-businesses-\\$17b-in-2019/d/d-id/1337035](https://www.darkreading.com/fbi-business-email-compromise-cost-businesses-$17b-in-2019/d/d-id/1337035)
- <https://www.zdnet.com/article/average-bec-attempts-are-now-80k-but-one-group-is-aiming-for-1-27m-per-attack/>
- <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/advanced-deception-with-bec-fraud-attacks/>
- <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019>
- <https://www.techrepublic.com/article/how-to-protect-your-organization-against-business-email-compromise-attacks/>



Questions



**Advanced Sources and Detector (ASD) Scorpius
Procurement Overview**

Michael P. Cisneros
Procurement Manager

October 8, 2020



The ASD Project Collaboration is a multi-site collaboration that capitalizes on the strengths of the partners



- Injector System – IVA
- Integrated Test Stand Support



- Solid State Pulsed Power
- Integrated Test Stand Support



- U1a Interface
- Integrated Test Stand Support



- Accelerator
- Detector
- Global Systems
- Integrated Test Stand
- Project integration and EVMS
- Downstream Transport System

In 2016, NNSA selected LANL as the lead for ASD

Our plan is to ‘under-promise’ and ‘over-deliver’ the capability in early FY25 – 4th QTR FY25 is the published commitment

TPC: \$500M-\$1100M

FPD EAC to CD-4: **\$885M**

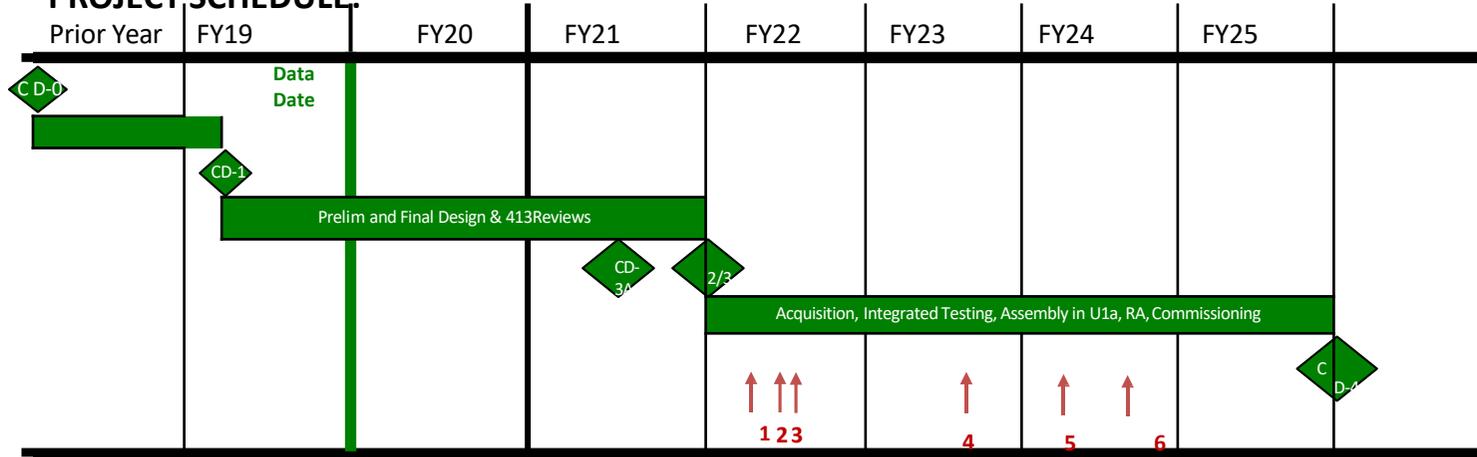
FPD Forecasted CD-4: Sept 2025

Project CD-4: Sept 2025

CPD EAC to CD-4: **\$691 M**

PM Forecasted CD-4: Sept 2025

PROJECT SCHEDULE:



UCEP/ASD Interproject Links

1. Ready to Install Equipment U1a.103, and Global Systems U1a.104 (December 2021)
2. Ready to Install Equipment U1a.102 (March 2022)
3. Ready to Install Accelerator U1a.104 (April 2022)
4. ZR Ready for Detector, Global Systems, other Diagnostics (May 2023)
5. ECSE Complex Ready for Testing (January 2024)
6. ECSE Complex Ready for Operation (July 2024)

Following the CD-3A submittal (October 2020), we plan on submitting CD-2/3 (March 2021) – procurements total ~\$300 M

- Planning of our procurements is critical to our success

Activity ID	Activity Name	Start	Finish	Budgeted Nonlabor Cost	2019	2020	2021	2022	2023
Total		01-May-19	15-Jan-25	\$297,126,954					
Los Alamos National Laboratory		01-May-19	15-Jan-25	\$117,545,397					
ASDSnap.1.02.02 Accelerator System (LANL)		01-May-19	17-May-23	\$56,216,686					
LAMTVS0100a	Module Vacuum Test Stand (MVTs)	13-Jun-19	18-Sep-19	\$213,850					
LAIVTS01100a	Injector-Accelerator Interface (IVTS)	26-Jul-19	06-Sep-19	\$195,520					
LAPAM101000	PAM Transport Magnets	12-Feb-20	22-Apr-20	\$126,929					
LAPAM100920	PAM Metglas	12-Feb-20	04-Jun-20	\$450,078					
LAPAM100930	PAM Compensation Cans	12-Feb-20	22-Apr-20	\$252,730					
LAPAM100940	PAM Global Systems Interface Components	12-Feb-20	22-Apr-20	\$265,887					
LAPAM100950	PAM Gap & Structured Machined Components	12-Feb-20	04-Jun-20	\$166,524					
LAPAM100960	PAM DAQ & Digitizers	12-Feb-20	25-Mar-20	\$155,623					
LAPAM100970	PAM PLCs	12-Feb-20	25-Mar-20	\$175,545					
LAPAM100980	PAM Steering Coil	12-Feb-20	22-Apr-20	\$154,871					
LAPAM100990	PAM Focusing Solenoid	12-Feb-20	22-Apr-20	\$141,088					
LA2020301-P001	IB Transport Magnet Coils	02-Sep-21	03-Mar-22	\$664,122					
LA2020301-P011	IB Transport Magnet Power Supplies	02-Sep-21	03-Mar-22	\$523,852					
LA202039701-P001	IB Alignment & Transport Stand	02-Sep-21	03-Mar-22	\$262,975					
LA2020122-P121A	Accelerator Cell Vacuum Controllers	02-Sep-21	11-Oct-21	\$310,839					
LA2020122-P131A	Accelerator Cell Vacuum Manifold & Bellows	02-Sep-21	17-Mar-22	\$706,297					
LAPROC10130	Accelerator Cell Forgings	16-Nov-20	03-Aug-21	\$1,177,171					
LA2020101-P014	Cell Block Cores Metglas PO	11-Mar-21	24-Aug-22	\$11,606,694					
LA2020101-P031	Cell Block Cores Insulator PO	20-Oct-20	24-Sep-21	\$941,942					
LA2020103-P014	Cell Block Focusing Solenoid Hollow Conductor PO	15-Mar-21	08-Nov-22	\$3,771,804					
LA2020104-P014	Cell Block Steering Coil Steering Chassis PO	15-Mar-21	26-Jan-22	\$3,911,152					
LAPROC10840	Accelerator Cell Ferrites	15-Mar-21	02-Feb-23	\$704,337					
LAPROC10740	Accelerator Comp Can Assemblies	15-Mar-21	10-Mar-23	\$7,741,477					
LAPROC10340	Accelerator Drive Plate Assemblies	15-Mar-21	22-Feb-23	\$1,926,980					
LAPROC10240	Accelerator End Plate	12-Apr-21	01-Mar-23	\$645,610					
LAPROC10440	Accelerator Gap Plate	15-Mar-21	22-Mar-23	\$1,814,211					
LAPROC10540	Accelerator Outer Housings	15-Mar-21	17-May-23	\$573,334					
LA2020122-P014	Cell Block Cell Vacuum Pumps PO	15-Mar-21	01-Aug-22	\$2,254,703					
LA202006-P014	Accelerator Data Acquisition and Controls Digitizers (Fast Diagnostics) PO	15-Mar-21	26-Jan-22	\$5,066,863					
LA202007-P014	Accelerator Data Acquisition and Controls PLCs (Slow Diagnostics) PO	15-Mar-21	26-Jan-22	\$5,714,204					
No ASD Award ID		01-May-19	03-Mar-22	\$3,599,476					

Keys to our success include establishing relationships, vendors in many technical areas (ITAR registration/ US Citizens)

- Unique fabrication/machining/production engineering
- Procurement Engineering services
- Electrical and Mechanical Designers with CREO experience
- Inventory and Production control software and services
- Logistical analysts to optimize supply chain and production
- Precision constant current power supplies (10-60 kW); high current at low voltage
- Solenoid magnets – water cooled
- Dielectric cables – coupling of pulsed power to cells
- Amorphous metal cores (e.g., Metglas)
- Vacuum systems (e.g., ion pumps, chemisorption and absorption pumps); ‘low energy’ pumps
- Electrical components (high current FETs, diodes, capacitors, etc.)



Questions



Strategic Sourcing Opportunities

Presenter:

Maureen Armijo, ASM Center of Excellence Team Leader

History

- **National Nuclear Security Administration (NNSA):**
 - Also known as National Security Enterprise (NSE)
 - Established by Congress in 2000
 - Part of the Department of Energy (DOE)
- **Supply Chain Management Center (SCMC):**
 - Part of NNSA and established in 2006
 - Founded to align purchasing power of Management and Operations (M&O) Contracting Sites (NNSA and EM only).
 - 80% of NNSA Acquisition Dollars passes through M&O Contractors
- **Integrated Contractor Purchasing Team (ICPT)**
 - Founded to align purchasing power of Management and Operations (M&O) Contracting Sites (NNSA, EM, Office of Science, other)
 - Agreements will need to have a sponsoring M&O contractor

SCMC IT initiatives

Category	Description	Type
IT	Managed Print Services	New
IT	Source to Pay (S2P)	New
IT	Dell	Recompete
IT	CISCO	Recompete

SCMC Fuel/Gas initiatives

Category	Description	Type
Fuel	Unleaded, Deiseal, e85	Recompete
Gas	Packaged Gas	Recompete

SCMC Professional Services Initiatives

Category	Description	Type
Professional Services	Architecture and Engineering Services	New (Multiple)
Professional Services	Recruitment Services	New
Professional Services	Safety Basis	Recompete
Professional Services	International Translation and Travel	Recompete

SCMC Operational Supplies Initiatives

Category	Description	Type
Operational Supplies	Electrical Supplies	Recompete

ICPT Initiatives

Description	Sponsoring Site
HVAC	ORNL
Supermicro	LANL
Electrical	Fermi/ANL
Siemens	SLAC
Analytical Laboratory Services	CHPRC
Office Supplies	Undecided

Description	Sponsoring Site
IT Equipment and Peripherals	ORNL
Managed Print Services	MSTS
Staff Augmentation	NREL/ ORNL/ SLAC/ ANL
Electronics	PNNL
Laboratory Test Equipment	INL

LANL Strategic Initiatives

Category	Description	Type
Maintenance, Repair and Operations	NQA-1 distributors	New (Multiple)
Software	Electronic Software Distribution (ESD)	Recompete



Questions



Multiple Award Task Order Contract (MATOC) Update

Presenter:

Susan Stein, Capital Projects

MATOC Update

Decontamination and Demolition (D&D)

- Consent granted October 5th
- Notification of Awardees in process

Modular Building

- Submitted for Consent, pending approval

Electrical

- Submission for Consent anticipated week of October 12th

Balance of MATOCs

- Award anticipated by December 30, 2020

MATOC Update

- Intent is to use the MATOCs for the majority of the work
- MATOC On boarding process
- Awardee Company/contact info posted on Opportunities Website
- Opportunities for Sub tiers may exist with MATOC Awardees.



Questions



Organizational Changes Capital Projects

Presenters:

Susan Stein & Brad Westergren, ASM Capital Projects

Organizational Changes

- Sue Stein moving to Capital Project Strategy and Logistics Planning
- A centralized role in the planning, coordination, and improvement initiatives related to Procurement for Capital Projects.
- Intersection of four critical areas:
 1. Strategic Planning
 2. Demand Management
 3. Subcontract Management Improvements
 4. Subcontractor Engagement



Closing Remarks

Presenter:

Yvonne Gonzales, ASM Small Business Program Office