Vulnerabilities and Social Engineering in Acquisition Scenarios

Clayton Boyer
Kathleen Hyatt
Mary Evans
Terry Leary
Zachary Levenson
Ryan Novak

May 8, 2024

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Research Question

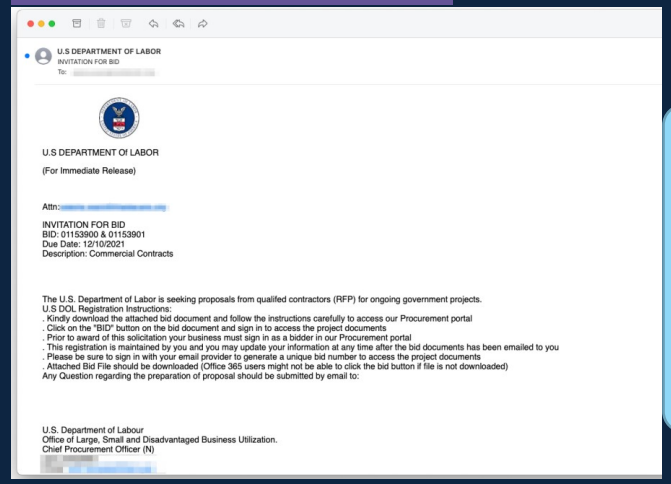
Social engineering activities, intelligence gathering, and supply chain threats are key tactics used by US competitors and adversaries.

How may these tactics be used to exploit Government Agency acquisitions?

MITRE

Operational Social Engineering: A Real-World Example

Phase 1: Investigation



U.S DEPARTMENT OF LABOR
INVITATION FOR BID
To:

U.S DEPARTMENT Of LABOR

(For Immediate Release)

Attn:

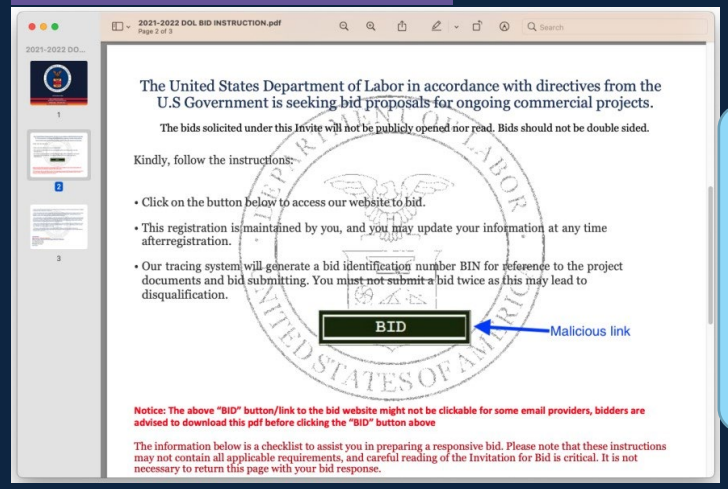
INVITATION FOR BID
BID: 01153900 & 01153901
Due Date: 12/10/2021
Description: Commercial Contracts

The U.S. Department of Labor is seeking proposals from qualifed contractors (RFP) for ongoing government projects.
U.S DOL Registration Instructions:
. Kindly download the attached bid document and follow the instructions carefully to access our Procurement portal
. Click on the "BID" button on the bid document and sign in to access the project documents
. Prior to award of this solicitation your business must sign in as a bidder in our Procurement portal
. This registration is maintained by you and you may update your information at any time after the bid documents has been emailed to you
. Please be sure to sign in with your email provider to generate a unique bid number to access the project documents
. Attached Bid File should be downloaded (Office 365 users might not be able to click the bid button if file is not downloaded)
Any Question regarding the preparation of proposal should be submitted by email to:

U.S. Department of Labour
Office of Large, Small and Disadvantaged Business Utilization.
Chief Procurement Officer (N)

Email sent with invitation to submit bids. Looks genuine, but upon closer inspection, note the different spelling of "Labour" vs. "Labor".

Phase 2: Hook



2021-2022 DOL BID INSTRUCTION.pdf

The United States Department of Labor in accordance with directives from the U.S Government is seeking bid proposals for ongoing commercial projects.

The bids solicited under this Invite will not be publicly opened nor read. Bids should not be double sided.

Kindly, follow the instructions:

- Click on the button below to access our website to bid.
- This registration is maintained by you, and you may update your information at any time afterregistration.
- Our tracing system will generate a bid identification number BIN for reference to the project documents and bid submitting. You must not submit a bid twice as this may lead to disqualification.

BID

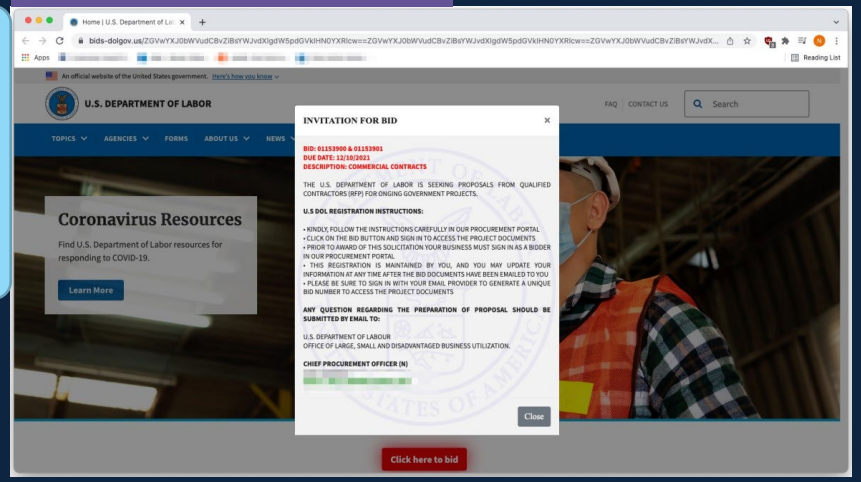
Malicious link

Notice: The above "BID" button/link to the bid website might not be clickable for some email providers, bidders are advised to download this pdf before clicking the "BID" button above

The information below is a checklist to assist you in preparing a responsive bid. Please note that these instructions may not contain all applicable requirements, and careful reading of the Invitation for Bid is critical. It is not necessary to return this page with your bid response.

Website where proposals are uploaded again looks genuine, however it contains a malicious link.

Phase 3: Play



U.S. DEPARTMENT OF LABOR

INVITATION FOR BID

BID: 01153900 & 01153901
DUE DATE: 12/10/2021
DESCRIPTION: COMMERCIAL CONTRACTS

THE U.S. DEPARTMENT OF LABOR IS SEEKING PROPOSALS FROM QUALIFIED CONTRACTORS (RFP) FOR ONGOING GOVERNMENT PROJECTS.

U.S DOL REGISTRATION INSTRUCTIONS:

- KINDLY, FOLLOW THE INSTRUCTIONS CAREFULLY IN OUR PROCUREMENT PORTAL
- CLICK ON THE BID BUTTON AND SIGN IN TO ACCESS THE PROJECT DOCUMENTS
- PRIOR TO AWARD OF THIS SOLICITATION YOUR BUSINESS MUST SIGN IN AS A BIDDER IN OUR PROCUREMENT PORTAL
- THIS REGISTRATION IS MAINTAINED BY YOU, AND YOU MAY UPDATE YOUR INFORMATION AT ANY TIME AFTER THE BID DOCUMENTS HAVE BEEN EMAILED TO YOU
- PLEASE BE SURE TO SIGN IN WITH YOUR EMAIL PROVIDER TO GENERATE A UNIQUE BID NUMBER TO ACCESS THE PROJECT DOCUMENTS

ANY QUESTION REGARDING THE PREPARATION OF PROPOSAL SHOULD BE SUBMITTED BY EMAIL TO:

U.S. DEPARTMENT OF LABOUR
OFFICE OF LARGE, SMALL AND DISADVANTAGED BUSINESS UTILIZATION.

CHIEF PROCUREMENT OFFICER (N)

Close

Coronavirus Resources

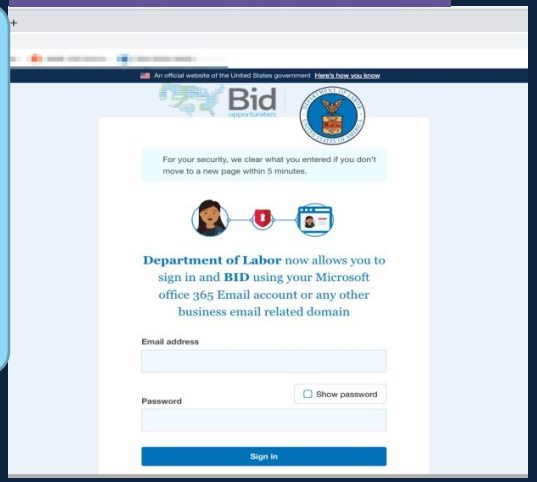
Find U.S. Department of Labor resources for responding to COVID-19.

Learn More

Click here to bid

Link asks the user to enter credentials in order to submit the bid. The malicious link has now provided access.

Phase 4: Exit



Bid

For your security, we clear what you entered if you don't move to a new page within 5 minutes.

Department of Labor now allows you to sign in and BID using your Microsoft office 365 Email account or any other business email related domain

Email address

Password

Show password

Sign in

The final stage; the Attacker now has unlimited access. Once credential are inputted, directs to "true" DOL sites to the user's MS 365 account and is provided

MITRE

Scenario 3: Market Research Information Gathering

Scenario:

- A malicious actor identifies the acquisition of interest
- The USG Agency posts RFI that include CS' email address on SAM.gov
- The malicious actor submits an email response to the RFI with a PDF attachment that contained malware
- The CS has unknowingly forwards the RFI response with a malicious attachment to the entire technical program team
  - At least one member clicks the link results in unauthorized backdoor access into the USG Agency network

Potential impact:

- The malicious actor combs through USG Agency system exfiltrating valuable health, personnel, and duty records
- The malicious actor is able to piece together sensitive operational details of the USG Agency
- The malicious actor is able to provide sensitive records back to their home country, including those who operated in their country

Recommendations:

- Move towards publicizing acquisition information in tightly controlled portals
- Vendors should be required to register for the portal and undergo a verification process before gaining access
- Each RFI/RFP published should also be limited based on 'need-to-know' basis based on NAICS codes or prior experience
- Measures allow for fair competition, while verifying Vendors and reducing risk of malicious actors accessing sensitive info

MITRE

Research Findings

- Completed 10 Unclassified and 15 Classified Scenarios to demonstrate potential acquisition vulnerabilities
- Research shows that Government acquisitions are most likely targets for social engineering activities, intelligence gathering, and supply chain threats
  - The potential acquisition attack surface area is large
  - There is a dichotomy between information security and Competition in Contracting Act
  - Hypothesis of the problem is ongoing, and the scale is much greater than the community realizes
- Examined the recommendations from all the scenarios to see what steps should be taken
- **Proposal:** The DoD community needs a process to assess and mitigate these threats
  - Current risk assessments focus on cost, schedule, performance of the supply or service
  - Acquisition Strategy Counterintelligence Risk Assessment (ASCRA) is a notional framework to meet this need but requires further development and refinement

Acquisition Strategy Counterintelligence Risk Assessment (ASCRA)

Risk Level	Recommended Countermeasures
ALL Acquisitions	- Improved social engineering and CI training for industry (specific examples such as malicious links, dangers of market research, etc.) - Improved social engineering and CI training for Gov't acquisition and security personnel - An assessment of the CI risk of an acquisition conducted during the acquisition strategy approval process that determines what the threat level and appropriate mitigations are.
Low	- SCRM / SBOM/ HBOM requirements for all IT purchases, and Labor contracts where software is created, modified, updated, etc - Non-IT: No action needed
Medium	All LOW measures plus use of: - Trusted vendor list, - Identification of critical components, - Supply chain attack reporting, - SCRM audits
High	All LOW and MEDIUM measures, plus use of: - Physically/logically separate market research site, - Pre-publication review and scrubbing publicly released announcements (J&A, sources sought, RFPs, etc.) - Limited blind sites for RFP material, - More rigorous subcontractor vetting

MITRE

We'd love to hear more about instances of social engineering attacks that you have encountered within your organizations. Please reach out to us!

Kathleen Hyatt
kbell@mitre.org

Zachary Levenson
zlevenson@mitre.org
https://www.linkedin.com/in/zack-levenson/

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE