Request for Information No 01
Date Received 03/17/2023

How many unique web applications are in the scope of this test?
There will be approximately 6-10 unique web application in the scope
Approximately how many active network devices (nodes) are running on the City's internal network?
Approximately 385
How many locations would you like visited for the social engineering portion of this assessment?
4 Site Locations
How many e-mails attempts and how many phone call attempts should be made?
This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 02
Date Received 03/17/2023

What is the anticipated date of award and contract execution?
Refer to 2.2 Project Timeline on the RFP
Is this a deliverable or time and materials-based contract? Deliverable
What is the total number of man hours required for this project?
This is a Request for Proposal, please make this part of your proposal if appropriate
What is the anticipated timeline for this project? After final vendor selection and award
What is the total number of resources which the client is expecting to work on this project?
Please let us know their position name (s) and maximum hourly rate(s)?
This is a Request for Proposal, please make this part of your proposal if appropriate
If only one candidate is required, can we propose multiple candidates as options (if one resource is unavailable post award, we can still go ahead with an alternate resource)?
This is a Request for Proposal, please make this part of your proposal if appropriate
Could you please share the job descriptions for each position needed to be staffed by vendors?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is there any budget allocated for this contract? If yes, can you please let us know the same?
Budget is under consideration
What is the maximum budget we can propose for this project?
This is a Request for Proposal, please make this part of your proposal if appropriate
Are hourly rate(s) acceptable for proposed personnel?
This is a Request for Proposal, please make this part of your proposal if appropriate
What is the maximum hourly rate we can propose for this project?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is the work entirely onsite or can it be done remotely to some extent?
This is a Request for Proposal, please make this part of your proposal if appropriate
Will the client allow candidates to perform work 100% remotely? No
How many people are currently working onsite and offsite for this project?
This is a Request for Proposal, please make this part of your proposal if appropriate
Will there be interviews post evaluation? Refer to 4.12 Deliverables on the RFP
If interviews are scheduled, will it be for the resource personnel only or for a team from the company including a company representative?
This is a Request for Proposal, please make this part of your proposal if appropriate
Could the client tell us when the project will be awarded, when it will start, and when the interviews will take place? Refer to 2.2 Project Timeline on the RFP
Could the client please clarify whether the post-vendor selection interview will be conducted in person or remotely? Refer to 4.12 Deliverables on the RFP
If in-person interviews are scheduled, can the client allow us to participate virtually? No
Considering the current COVID-19 pandemic situation, if the proposed candidates are not available at the time of award, will the agency allow us to provide replacement personnel with similar or more skill sets? No
If we are shortlisted for an interview and if our proposed personnel are not available at that time, can we propose alternate resources for the interview? No

Request for Information No 03
Date Received 03/20/2023

How many hosts are part of this breakdown? Approximately 200
Also, how many users? 200
How many DNS name? Will be provided before testing
How many web app? There will be approximately 6-10 unique web application in the scope
How many roles for each web app? Will be provided before testing
(customer, patient, taxpayer, other) please confirm what is other? Will be provided before testing
Please confirm number of sites? 4 Site Locations

_____

Request for Information No 04
Date Received 03/20/2023

With regards to the external penetration test (Page 8, Section 4.6), do all in scope public facing IP addresses belong to the City of San Dimas, or are any systems hosted by/IPs belonging to a 3rd party? (For example, Amazon Web Services, Google Cloud Platform, etc.) 1 website is hosted by 3rd party
How many web applications are to be included in the testing?
There will be approximately 6-10 unique web application in the scope
What is the purpose of each of the applications? Will be provided before testing
Are the applications Commercial Off the Shelf (COTS), or custom coded by a 3rd party, or custom coded in house? COTS
What software or coding languages are used? (i.e. PHP, .net, perl, java, javascript, Go, python, compiled)
Will be provided before testing
How many unique dynamic pages (pages that change based on user inputs)? (e.g., an e-commerce site that sells products may have hundreds of dynamic pages, but each dynamic page is the same underlying code) For scoping purposes, only provide the number of unique pages with dynamic content for each application.
Will be provided before testing
Is authenticated testing being requested? If yes, will test credentials be provided?
Refer to 4.8 Network Security Assessment on the RFP
Will be provided before testing
How many and what types of user roles would you like tested, for each application?
Will be provided before testing

With regards to the network security assessment, also known as an internal penetration test based on the provided description (Page 9, Section 4.8), is it the preference of the City of San Dimas that this internal network pen testing be performed on site, or can it be done entirely remote? We do understand that there is an on-site component for social engineering (Page 9, Section 4.10), which we would typically come on site for X number of days to accomplish the goals of a physical pen test and the in person tactics for social engineering, while doing the network based testing remotely. Is this acceptable, to reduce the amount of time on-site, and thus travel cost?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many physical buildings will be included in scope? 4 Site Locations
Are there armed security guards or law enforcement present at these buildings? No
Will physical security assessment/on-site social engineering be conducted solely during or after business hours, or both? During Business Hours M-F 8-4p
With regards to the findings presentation as a part of the Deliverables (Page 10 & 11, Section 4.12), will the City of San Dimas require that the penetration testers be physically present for this onsite meeting, or would it be acceptable to share the results via an online format such as Zoom or MS Teams?
Refer to 4.12 Deliverables on the RFP
This is a Request for Proposal, please make this part of your proposal if appropriate
With regard to the bullet in the General Requirements (Page 7, Section 4.5) that describes that all testing is expect to be performed within 10 continuous business days, how firm is the City of Dimas on this? While the

external and internal network pen tests seem to be pretty straightforward in terms of being able to estimate efforts, the answers to the above questions for web application penetration testing and physical security testing could drastically increase the time needed.
This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 05
Date Received 03/21/2023

Approximately how many external IPs are in scope? Approximately 50
Please confirm both External and Internal Vulnerability Assessments and Penetration Tests are in scope Yes
Do the 50 IP addresses specified also represent the device count? No
Does 50 Internal IPs include both servers and end user devices? No
Does the scope of the physical security assessment include a single location/building or multiple location? 4 Site Locations

_____

Request for Information No 06
Date Received 03/22/2023

Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance? -No
Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project? Budget is under consideration
Specify the VLAN details how many are included in the Scope? Approximately 7
Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)? Will be provided before testing
How much (%) of the infrastructure is in the cloud? Very low percentage
In the IT department/environment, how many employees work? 2 Full Time Employees
Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? Own

_____

Request for Information No 07
Date Received 03/22/2023

In section 4.2 (page 6), it states there will be two tests annually. However, sections 4.6-4.10 show 5 phases for the engagement. Is it acceptable to provide pricing and scheduling for each of these 5 phases, rather than two separate tests? This is a Request for Proposal, please make this part of your proposal if appropriate
How many applications are in scope for testing?
There will be approximately 6-10 unique web application in the scope
Can you list the applications/give an idea as to the size of each application (number of web pages for example) to help scope the assessment? Will be provided before testing
If more than one application, is a comprehensive assessment of each required?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many servers, desktops, firewalls, network devices, etc. are in scope for this test?
Will be provided before testing
Is onsite wireless infrastructure expected? Yes
If so, how many locations require wireless assessments? How large is each building?
4 Site Locations - Will be provided before testing
If wireless testing is not required, is it okay to propose that this section of services be performed remotely?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many offices/buildings are in scope for this assessment? Can you provide the address of the locations for assessment so that we can scope the assessment? 4 Site Locations - Will be provided before testing

_____

Request for Information No 08
Date Received 03/23/2023

How many public-facing IP addresses (IP Ranges) are there for external vulnerability and penetration testing? Please also provide the number of public IP addresses in use. Approximately 12
How many public-facing web sites and/or applications are there for external vulnerability and penetration testing? Please provide the number of web sites/applications and/or the specific URLs.
There will be approximately 6-10 unique web application in the scope
Will be provided before testing
What is the complexity level for the public-facing websites/applications (e.g. tiers, number of pages, number of input forms, authentication, backend database, etc.)? Will be provided before testing
For application security testing, we can also conduct more in-depth vulnerability testing and/or code analysis. Are these services required?
This is a Request for Proposal, please make this part of your proposal if appropriate
Are any of the public IP addresses or web sites hosted by a third party? 1 website is hosted by 3rd party
Typically, we conduct a basic phishing exercise as part of the penetration test in order to test both the technical and people-related risks. Is this something that you would be interested in?
Refer to 4.9 Physical Security Assessment on the RFP
We can also perform vulnerability scanning to identify vulnerabilities of internal systems (patching levels, ports, services), is this service required? If yes, how many private IP addresses would be in scope? Approximately 7 /24 subnets
Can the application be accessed over the internet? Yes
Can our testers create their own accounts, or will it require client-provided credentials?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is the application behind a Web Application Firewall? Will be provided before testing
Please provide the URL(s) to be tested? Will be provided before testing
What is the address of each building to be assessed from a physical security perspective.
4 Site Locations - Will be provided before testing
Approximate square footage/floors and number of occupants (city employees/contractors or mix), city-owned or leased. Will be provided before testing
Nature of business at each location to be assessed, office, warehouse, maintenance, vehicle garage, etc.
Will be provided before testing
General number of exterior access points at each facility to be assessed.
Will be provided before testing
Number of server rooms in each facility to ascertain physical security of those server rooms.
Will be provided before testing
Security system integration platform currently in use (if any), door controls, alarm system, ID card system for access control., surveillance camera system. Will be provided before testing
Do physical security/access control policies and procedures exist city-wide or for each specific location. If so, we will review what is in place and make recommendations. If not, it can be very time-consuming if you want us to help develop policies and procedures.
This is a Request for Proposal, please make this part of your proposal if appropriate

Request for Information No 09
Date Received 03/23/2023

Can the project be split into different phases?
This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 10
Date Received 03/24/2023

Can you provide context as to how large the building for assessment is? How many rooms, floors, etc.?
Will be provided before testing

Are the web applications internal or external facing? Will be provided before testing
Are there apps that are in-house tools only? Will be provided before testing

_____

Request for Information No 11
Date Received 03/24/2023

Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days.
Are you asking how much we can do in the 10 days or what the total timeframe that it will take us to do the entirety of the work. This is a Request for Proposal, please make this part of your proposal if appropriate
Results of Vendor's employees background check(s) (each employee shall have a clean background record).
What kind of background check specifically are you asking for? Is this with the city or FBI background check? The company would be glad to provide this once the contract has been awarded. Can we provide that at that time? This is a Request for Proposal, please make this part of your proposal if appropriate
Will San Dimas provide, in writing, notification to law enforcement of the physical security assessment?
Will be provided before testing
Does the entire staff need to be at the onsite meeting for the meeting, or might an officer of the company attend with supporting staff joining remotely?
This is a Request for Proposal, please make this part of your proposal if appropriate
Relevant Industry Certifications
Do you want the resumes here?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is San Dimas open to the following payment terms?
Can the city make a 50% payment be made by the city once an agreed upon price is set before work starts? The remaining balance (50%) be paid within 30 days net after all of the work has been completed, materials delivered, and briefings finished according to the terms of the Statement of Work and satisfaction of the staff. Travel and Expense be billed separately and due immediately upon invoicing as a portion of this engagement will need to be completed onsite. The company will be glad to provide receipts for the costs that were incurred. This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 12
Date Received 03/24/2023

Is the IT organization centralized or decentralized? Centralized
What is the County of San Dimas budget for this project? We are not County
Budget is under consideration
Has the County of San Dimas had this type of penetration testing performed in the past? No
As an organization, are you confined to awarding to the lowest bidder? No
Approximately how many IPs are active? Approximately 12
Is exploit testing included in the external network vulnerability scans? Yes
How many web applications are in scope?
There will be approximately 6-10 unique web application in the scope
Are the web applications Internet-facing or internal only? Will be provided before testing
Can all internal network testing be done from a single location? No
Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?
Will be provided before testing
How many routers | switches are in scope for a configuration review?
Will be provided before testing
Is San Dimas open to sample-based testing?
This is a Request for Proposal, please make this part of your proposal if appropriate

How many enterprise applications are in scope? Will be provided before testing
Are the enterprise applications COTS or internally-developed? COTS
How many unique databases are in scope for database-specific testing? Will be provided before testing
If databases are in different locations, can all locations be reached from one central location? Yes
How many unique server brands are in scope for testing? Will be provided before testing
What devices does the Security Configuration Review cover?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is the wireless network controller-based or access-point-based?
Will be provided before testing
How many locations are in scope for wireless network testing? 4 Site Locations
How many targets are anticipated for each type (Phishing, Vishing, Spear Phishing, Business Email Compromise, Whaling, Pre-Texting) of testing?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many endpoints are in scope? Approximately 385

Request for Information No 13
Date Received 03/24/2023

Is there an authenticated portion of the application that will be included within testing scope?
Approximate number of pages?
Approximate number of input fields?
This is a Request for Proposal, please make this part of your proposal if appropriate
Number of hosts involved in serving the application (application servers, database servers, etc.)?
Approximate number of application users?
Number of user roles to be tested?
Approximately 200
Will application testing be performed in production or within a testing environment? Production
Is the application hosted on-premise or by a hosting provider? Will be provided before testing
What are the primary programming languages used by the application?
Will be provided before testing
Are there any mobile applications to be included? if yes, please complete below: No
Is iOS included?
Is Android included?
Is there access to APK, and IPA application files?
If a 3rd party is involved: (ignore if not applicable) No
Can we get third party approval for testing?
Can we get credentials for credentialed testing?
Additionally, if you can confirm the number of physical locations that will be in scope for onsite physical assessments or onsite social engineering assessments, that would be appreciated.
4 Site Locations
Lastly, if you can confirm for me whether wireless networks will be in scope for this project, that would also be helpful. Refer to 4.8 Network Security Assessment on the RFP
If Wireless Network testing is in scope, please answer the following:
What is the number of wireless access points? Will be provided before testing
What is the number of wireless access controllers? Will be provided before testing
What is the number of WIFI networks, aka number of SSIDs? 4 SSID
What is the number of locations? (Although BPM performs this service remotely, it is helpful to know number of locations) 4 Site Locations

Request for Information No 14
Date Received 03/27/2023

Kindly provide a brief on the inventories for City's IT infrastructure. Will be provided before testing
Is this a new initiative? If not, please enlist the incumbent vendor(s). Yes
How many agencies do City intend to award the contract? 1
What is the budget for this contract? Budget is under consideration
What was the previous spending of the contract (if any)? N/A
Can you please provide a pricing template? N/A

_____

Request for Information No 15
Date Received 03/27/2023

(Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) (continuous business days). Are we expected to complete the assessment within 10 days? –
This is a Request for Proposal, please make this part of your proposal if appropriate
Total number of Internal IP addresses Will be provided before testing

No. & Type of Assets Will be provided before testing
Servers Will be provided before testing
Network Devices Will be provided before testing
Routers Will be provided before testing
Switches Will be provided before testing
Storage Will be provided before testing
Load balancers Will be provided before testing
Firewalls Will be provided before testing
Database's Will be provided before testing
OS Windows Environment
Are there any OT devices that need to be scanned? Will be provided before testing
Types Will be provided before testing
Connectivity to the network Will be provided before testing
No. of OT Devices Will be provided before testing
For external scanning would this be an authenticated or unauthenticated scan? Both
Is there a specific time when scans should be performed?
This is a Request for Proposal, please make this part of your proposal if appropriate
What is the business requirement for this penetration test?
Security Penetration Testing Services
When was the last VA/PT performed?
Will be provided before testing
Does the resource need to be onsite for this engagement? Onsite
If remote, any restrictions on it being offshore v/s offsite v/s onshore?
This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 16
Date Received 03/27/2023

Does the city have a preference as to each of the five phases above to be included in either the External or Internal Penetration Test or shall we propose which of the five phases should be performed during either the External or Internal Penetration Testing?
This is a Request for Proposal, please make this part of your proposal if appropriate
Data is obtained during the penetration test and the data (evidence) may be included in the final report. We will require access to the data for report writing, which may require temporarily storing the data until the report and project phase is complete. The data will be returned and scrubbed from our penetration testing equipment after the project phase is complete. Is this acceptable to the City? Acceptable
What are the City's requirements for background checks?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many personnel does the City require to be subjected to social engineering testing? Of the above social engineering methods, does the City have a preference on what methods should be performed or does the City require all methods to be performed?
This is a Request for Proposal, please make this part of your proposal if appropriate
Will the City accept electronic proposals? No
If the City cannot accept electronic proposals, will the City grant a one-week extension to the due date to allow time for printing and shipping? No

Request for Information No 17
Date Received 03/27/2023

How many Windows Domains are in use at San Dimas that will be in scope? 1
How many subnets will be in scope for the internal portion of the assessment? Will be provided before testing
Counting all live IPs on all in-scope subnets, will there be more than 50 live IPs on the Sam Dimas internal network? Yes
For the physical security assessment, how many physical buildings does San Dimas operate out of that will be in scope? How many personnel in total work on-site? 4 Site Locations

_____

Request for Information No 18
Date Received 03/27/2023

How many web applications are in the scope of test?
There will be approximately 6-10 unique web application in the scope
How many dynamic pages does each application contain? Will be provided before testing
How many user roles are to be tested for each application? Will be provided before testing
If application make calls to internal APIs, then how many API endpoints are in the scope of test?
Will be provided before testing
How many internal applications are in the scope? Will be provided before testing
How many dynamic pages does each application contain? Will be provided before testing
How many user roles are to be tested for each application? Will be provided before testing
Count of Domain Controllers in scope? Will be provided before testing
Count of Internal web servers in scope? Will be provided before testing
Count of DMZ network in scope? Will be provided before testing
Count of Wireless devices in scope? Will be provided before testing
Can all wireless devices be reached from one location? Yes
If yes, how many floors are there in the building? N/A
If not, how many locations needs testing and number of floors on the building? Will be provided before testing
Count of internal private IP addresses in scope? Will be provided before testing
Count of other network devices in scope and their names? Will be provided before testing
How many Physical locations are in the scope of 'Physical Security Assessment'? 4 Site Locations
Are you looking at Red Team Assessment type of engagement for this?
This is a Request for Proposal, please make this part of your proposal if appropriate
Will review of physical security control policies and procedures documents also part of this assessment?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many estimates users are to be tested? Will be provided before testing
'Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days.' *– Are you looking for not more than 10 days for each assessment to be completed?* Kindly elaborate this statement.
This is a Request for Proposal, please make this part of your proposal if appropriate
For Security Assessments and Penetration testing, are there any tool preference, like only commercial security tools, no open source tools, etc.
This is a Request for Proposal, please make this part of your proposal if appropriate
In Section 2.4 for the RFP it is mentioned that "*All inquiries received before the deadline will be compiled and responses to inquiries will be posted on the City of San Dimas website, located at sandimasca.gov. All inquiries so issued shall become part of the Contract Documents."* Could you please suggest under which category tab we shall be able to locate the Contract Documents? Request For Proposals For Security Penetration Testing Services (sandimasca.gov)

Request for Information No 19
Date Received 03/27/2023

Has this project been conducted before? If so, who is the incumbent? No
What is the anticipated budget for this project? Budget is under consideration
Does the City have an anticipated start time for this project? Soon after final vendor selection and award
Does the City have an anticipated completion date for this project? To be determined
For clarification: when the City says “Vendor shall specify the ability to perform and complete External, Internal, Web Application, Physical Security and Social Engineering tests within Ten (10) continuous business days,” does this mean that the City wants all 5 assessments to be completed within 10 continues business days, or does each individual assessment have 10 days to be completed?
This is a Request for Proposal, please make this part of your proposal if appropriate
For clarification: when the City states “Vendor must be able to provide complimentary post-remediation reviews (Discussion-Based)” on page 7, does this mean that the City is looking for a meeting to discuss the findings? If so, how many?
This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 20
Date Received 03/27/2023

For the wireless network assessment and penetration testing, how many wireless networks (distinct SSIDs) will be in scope? 4 SSID
Will there be employees in the office to generate authentication traffic? Yes
For internal penetration testing, would the CLIENT like us to focus our "attack and exploit", how many servers, desktops, firewalls, network devices will be in scope?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is private and guest the only wireless networks (distinct SSIDs) that are in scope of penetration testing? No
Will the [SCADA ICS/CJIS, etc.] environment be in scope for penetration testing or is only a review of controls required? No
Is retesting desired? This is a Request for Proposal, please make this part of your proposal if appropriate
Can you please provide the names of the critical applications in use? Will be provided before testing
Are any of the critical applications custom developed? If yes, which are they? No
How many application roles does the CLIENT want tested for each web application during web application penetration testing? This is a Request for Proposal, please make this part of your proposal if appropriate
How many user roles per web application would CLIENT like us to test for credentialed scanning for each of the _____ public facing sites and _____ internal sites?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many user roles per web application would CLIENT like us to test for credentialed scanning for each of the _____ public facing sites and _____ internal sites?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many pages are contained in the application?
With user input forms?
Without user input forms?
What request data is sent to the server throughout the application?
Number of data form fields
Number of cookies
List of header tags used
Numbers of JSON fields
Does the site use Authentication?
Backend authentication mechanism
Number of user roles in the application
Are there any web services?
If so, how many endpoints and what technology is used?
How many APIs are to be tested with each web application that is in scope?
For web applications penetration testing, does CLIENT want API testing to be included? If yes -
Total number of APIs

Total number of unique requests for all APIs (if they don't have this we could get an idea of endpoint count and work from there)

Is the API defined?

Is there API documentation?

Is there a specification or a collection?

What is the approach?

Blackbox/Greybox/Whitebox

Authenticated/authorized testing?

The above will be provided before testing

For the social engineering component, how many phone-based vishing attack campaigns does the CLIENT desire? How many target individuals are expected to be called for each vishing campaign? Over how many weeks does the CLIENT want each vishing attack to run?

This is a Request for Proposal, please make this part of your proposal if appropriate

For phone phishing, how many targets/samples will be tested? How many rounds of attempts?

What is the number of email phishing campaigns desired by the CLIENT? (A campaign is a single email blast using uniform email content.)

This is a Request for Proposal, please make this part of your proposal if appropriate

_____

Request for Information No 21
Date Received 03/27/2023

Please provide a list of in-scope URLs or a quantity number for the web application tests.
There will be approximately 6-10 unique web application in the scope
On page 7 - Section 4.5 of the RFP, it states that the vendor must specify the ability to perform and complete the External, Internal, Web Application, Physical Security, and Social Engineering tests within Ten (10) continuous business days. Is the ability to complete everything in 10 days a requirement to respond to the RFP?
This is a Request for Proposal, please make this part of your proposal if appropriate
Can we use sub-contractors to do portions of the review? No

Request for Information No 22
Date Received 03/27/2023

We understand that you have requested the responses to be submitted in Hard Copies, would the agency accept an electronic RFP Submission instead of a hard copy submission? No
Is there any mandatory number of references we have to provide?
This is a Request for Proposal, please make this part of your proposal if appropriate
Are there any mandatory Industry Certifications we must have?
This is a Request for Proposal, please make this part of your proposal if appropriate
If we don't have any Industry Certification we will be disqualified?
This is a Request for Proposal, please make this part of your proposal if appropriate
How many web applications will be targeted during this phase?
There will be approximately 6-10 unique web application in the scope
Will the testing be authenticated using provided credentials, or unauthenticated testing only?
Refer to 4.8 Network Security Assessment of the RFP
If authenticated, how many user role types are defined within the application?
Will be provided before testing
What is the approximate size of the local area network in total active IP Approximately 200
Will credentials be provided for authenticated vulnerability scanning?
Will be provided before testing
How many offices does the City of San Dimas operate? 4 Site Locations
How many employees will be targeted for social engineering attacks?
This is a Request for Proposal, please make this part of your proposal if appropriate
The solicitation document does not include a pricing format, Does the city have a preferred pricing format? If not, can we use an excel spreadsheet detailing milestones and the cost of each?
This is a Request for Proposal, please make this part of your proposal if appropriate
Does the city have a desired font size and type for us to present our proposal? No
Is there a page limit for our response? No
What is the estimated budget available for the end-to-end of the project? Budget is under consideration
Could the agency please grant an extension on the due date? No
If we are using a subcontractor, can the subcontractor meet the minimum requirements? No
If the resources we provide at the time of proposal submission are not available at the time of a potential contract award could we replace them with equally qualified resources? No
Does the agency accept remote resources to work on the project?
This is a Request for Proposal, please make this part of your proposal if appropriate
Does the agency prefer on-site resources to execute the project?
This is a Request for Proposal, please make this part of your proposal if appropriate
Is there any incumbent associated with this project? If so, please disclose the name. No
Does the agency require wet ink signatures? No
Is it allowed to use digital signatures? Yes
Is it required to provide the COI alongside the proposal response? Yes

Does the agency have a percentage established for MBE/DBE/WBE? Please make this part of your proposal.
If we are using a subcontractor, can the subcontractor meet MBE/DBE/WBE participation? No

_____

Request for Information No 23
Date Received 03/27/2023

Has the City of San Dimas previously performed a penetration test? If yes, how many times and when? No
Is there an incumbent providing similar services to the City of San Dimas? If yes, is the incumbent performing to the satisfaction of the City and the Information Systems Manager? Is the incumbent eligible to bid on this contract? No
Will the City be permitting penetration testing to be performed by existing or previous managed IT or managed service providers? Or will the City be requiring third-party independence to reduce the risks of conflict of interests or the optics of "grading one's work" ? No
Will Vendors be permitted to use off-shore teams to perform and/or support any and all penetration testing activities? No
On page 6, In Section 4.2, the RFP states "The proposed schedule should include planning for two tests annually, one external penetration test and one internal penetration test." Is our understanding correct that the City is looking for two external and two internal penetration tests, with a pair of tests conducted roughly six months apart?
This is a Request for Proposal, please make this part of your proposal if appropriate
On Page 6, Section 4.2, the RFP states "The proposed schedule should include planning for two tests annually, one external penetration test and one internal penetration test."
This is a Request for Proposal, please make this part of your proposal if appropriate
On Page 8, Section 4.6, we see the requirements and expectations for External Network Penetration Test.
This is a Request for Proposal, please make this part of your proposal if appropriate
Could one direct us to the requirements and expectations for Internal Network Penetration Test?
This is a Request for Proposal, please make this part of your proposal if appropriate
On Page 9, Section 4.8 – Network Security Assessment, there are mentions of a "penetration style test" and "internal network vulnerability assessment" in the same paragraph. Could the City provide additional context and details to the expectations and outcomes of a "penetration style test" because "penetration style test" is not something we have seen or heard before?
This is a Request for Proposal, please make this part of your proposal if appropriate
On Page 9, Section 4.8 – Network Security Assessment, we want to confirm that security exploits may be executed as part of the network security assessment.
This is a Request for Proposal, please make this part of your proposal if appropriate
On page 6, In Section 4.2 – For both the internal penetration test and external penetration test, we want to confirm that the expectation is that manual testing is expected and not simply a Vendor running a Qualys, Nessus, or some other automatic vulnerability assessment tool and providing the tool output to the City.
This is a Request for Proposal, please make this part of your proposal if appropriate
On page 7, under the General requirements, it states that "Vendor shall not store any data, if obtained during a penetration test." We have a concern that if the City does not allow the vendor to store any data, the Vendor would potentially be in breach of contract. By the plain language reading of that requirement, a Vendor would not be able to conduct any level of testing, collect any data, and collect information necessary for reporting and artifacts for the City. Would the City permit the Vendor to reasonably store information that's necessary for reporting? Yes

On page 7, under the General Requirements, it states that the Vendor shall supply a list of potential employees, including their "Relevant Industry Cyber Security Certifications.". Does the City have any preferred Industry Cyber Security Certifications it is looking for? (e.g. Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP))

This is a Request for Proposal, please make this part of your proposal if appropriate

On Page 9, Section 4.8 – Network Security Assessment, could we confirm that the City of San Dimas' PSAP (Public Safety Answer Point) is in scope? If yes, could we also confirm that Next-Generation 9-1-1 is in scope?

Not in scope

On Page 8, Section 4.7, Web Application Penetration Test, could the city detail how many web applications are in scope?

There will be approximately 6-10 unique web application in the scope

How many applications are internet facing? How many applications are internal only?

Will be provided before testing

Could the City detail the expectation of how comprehensive and detailed the web application penetration test is expected to be?

This is a Request for Proposal, please make this part of your proposal if appropriate

On Page 8, Section 4.7, Web Application Penetration Test, we want to confirm that the expectation is that manual testing is expected and not simply a Vendor running a Qualys, Nessus, or some other automatic vulnerability assessment tool and providing the tool output to the City.

This is a Request for Proposal, please make this part of your proposal if appropriate

On Page 13, Section 6.5, could the city specify the number of references it expects as part of the submission?

This is a Request for Proposal, please make this part of your proposal if appropriate