# Phần 2. YÊU CẦU VỀ KỸ THUẬT

# Chương V. YÊU CẦU VỀ KỸ THUẬT

## 1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Tên dự toán: Thuê dịch vụ kiểm tra, đánh giá an toàn thông tin cho hệ thống thông tin, phần mềm.

- Tên gói thầu: Thuê dịch vụ kiểm tra, đánh giá an toàn thông tin cho hệ thống thông tin, phần mềm.

- Chủ Đầu tư: Cục Công nghệ thông tin - Bộ Tư pháp.

- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi trong nước, qua mạng.

- Phương thức lựa chọn nhà thầu: Một giai đoạn một túi hồ sơ.

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện hợp đồng: 60 ngày.

- Địa điểm thực hiện: Cục Công nghệ thông tin - Bộ Tư pháp, số 60 Trần Phú, phường Ba Đình, thành phố Hà Nội

## 2. Mục tiêu công việc:

Thuê dịch vụ Kiểm tra, đánh giá an toàn thông tin cho hệ thống thông tin tại Trung tâm dữ liệu điện tử Bộ Tư pháp nhằm đáp ứng các yêu cầu về bảo đảm an toàn thông tin theo quy định của pháp luật, phát hiện sớm các rủi ro, lỗ hổng tiềm ẩn tồn tại trên hệ thống CNTT của Bộ. Trên cơ sở đó, khuyến cáo, đề xuất phương án và tiến hành khắc phục các lỗ hổng được phát hiện.

## 3. Yêu cầu kỹ thuật của gói thầu:

*3.1. Yêu cầu chung:*

- Nhà thầu chứng minh quyền sử dụng hợp pháp đối với công cụ đánh giá thương mại hoặc công cụ đánh giá tự phát triển.

- Nhà thầu có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng được đơn vị có thẩm quyền cấp.

- Báo cáo kết quả kiểm tra, đánh giá cần thể hiện đầy đủ các nội dung thông tin về đối tượng đánh giá, danh sách các lỗ hổng, mức độ ảnh hưởng, các khuyến nghị, hướng dẫn khắc phục các lỗ hổng, nguy cơ.

- Bên cung cấp dịch vụ có hỗ trợ thực hiện kiểm tra đánh giá lại sau khi các lỗ hổng, nguy cơ đã được khắc phục, để đảm bảo việc khắc phục đã được thực hiện thành công.

- Các thông tin mà phía chủ đầu tư cung cấp cho nhà thầu, bao gồm các tài liệu thiết kế, thông tin tài khoản, danh sách thiết bị, kết nối VPN,… chỉ được sử dụng cho mục đích thực hiện gói thầu và chỉ được sử dụng trong thời gian thực hiện gói thầu.

- Mọi thông tin mà phía nhà thầu thu thập được trong quá trình tấn công, kiểm thử hệ thống phải thông báo lại cho phía chủ đầu tư. Phía nhà thầu đảm bảo việc chỉ thu thập dữ liệu ở mức tối thiểu đủ để chứng minh tác động của lỗ hổng, nguy cơ, và việc thu thập dữ liệu chỉ để phục vụ mục đích chứng minh tác động của lỗ hổng, nguy cơ. Sau khi hoàn thành việc kiểm tra, đánh giá nhà thầu cần đảm bảo việc không còn lưu trữ các dữ liệu thu thập được, đồng thời chịu trách nhiệm nếu các dữ liệu này bị tiết lộ cho bên thứ ba.

- Các báo cáo, kết quả kiểm tra đánh giá là tài sản của chủ đầu tư và cần được bảo mật. Nhà thầu không được phép tiết lộ chi tiết kết quả đánh giá của chủ đầu tư cho bên thứ ba khi chưa có sự cho phép của chủ đầu tư.

- Danh mục các hệ thống đánh giá:

| Stt | Tên hệ thống | Đơn vị tính | Số lượng |
|---|---|---|---|
| **I** | **HỆ THỐNG THÔNG TIN PHẦN MỀM, ỨNG DỤNG** | | |
| **1** | **Cổng thông tin điện tử Bộ Tư pháp** | Ứng dụng | 1 |
| | Kho lưu trữ images:<br>https://k8sregistry.moj.gov.vn | | |
| | Xác thực:<br>https://portalauth.moj.gov.vn | | |
| | Media:<br>https://portalmedia.moj.gov.vn | | |
| | Phân tích người dùng:<br>https://portalanalytics.moj.gov.vn | | |
| | Cổng thông tin điện tử Bộ Tư Pháp:<br>https://moj.gov.vn | | |
| | Trang tin bộ trưởng:<br>https://botruong.moj.gov.vn | | |
| | Trang thi hành án dân sư:<br>https://thads.moj.gov.vn | | |
| | Trang Thông tin Bổ trợ tư pháp:<br>https://bttp.moj.gov.vn | | |
| | Trang Thông tin Công nghệ thông tin:<br>https://cntt.moj.gov.vn | | |
| | Trang Thông tin Công tác cán bộ và Thi đua khen thưởng:<br>https://thiduakhenthuong.moj.gov.vn | | |

| Stt | Tên hệ thống | Đơn vị tính | Số lượng |
|---|---|---|---|
| | Trang Thông tin Viện Chiến lược và khoa học pháp lý:<br>https://khpl.moj.gov.vn | | |
| | Trang Thông tin Xây dựng pháp luật:<br>https://xdpl.moj.gov.vn | | |
| | Trang Thông tin Hợp tác quốc tế về pháp luật:<br>https://hoptacquocte.moj.gov.vn | | |
| | Trang Thông tin Cải cách tư pháp và hoạt động tư pháp:<br>https://cctphdtp.moj.gov.vn | | |
| | Kho dữ liệu truyền thông (UI):<br>https://mediastore.moj.gov.vn | | |
| | Trang Thông tin Pháp luật quốc tế:<br>https://plqt.moj.gov.vn | | |
| | Trang Thông tin Cải cách hành chính:<br>https://cchc.moj.gov.vn | | |
| | Trang thông tin Hành chính tư pháp:<br>https://hanhchinhtuphap.moj.gov.vn | | |
| | Trang thông tin Đăng ký biện pháp bảo đảm và Bồi thường nhà nước:<br>https://dkgd.moj.gov.vn | | |
| | Trang thông tin Cục Kiểm tra văn bản và Quản lý xử lý vi phạm hành chính:<br>https://ktvb.moj.gov.vn | | |
| | Trang Thông tin Đảng đoàn thể:<br>https://ddt.moj.gov.vn | | |
| | Trang Thông tin Tuổi trẻ Bộ Tư pháp:<br>https://tuoitrebtp.moj.gov.vn | | |
| | Trung tâm thông tin và dịch vụ:<br>https://ttcndv.moj.gov.vn/ | | |
| | Trang kiểm soát thủ tục hành chính:<br>https://kstthc.moj.gov.vn | | |
| | Trang Thông tin Pháp luật trong kỷ nguyên mới:<br>https://pltknm.moj.gov.vn | | |

| Stt | Tên hệ thống | Đơn vị tính | Số lượng |
|---|---|---|---|
| | Trang tin thứ trưởng T.T Nguyễn Thanh Tịnh: https://ttnguyenthanhtinh.moj.gov.vn | | |
| | Trang tin thứ trưởng T.T Đặng Hoàng Oanh: https://ttdanghoangoanh.moj.gov.vn | | |
| | Trang tin Phó Bí thư chuyên trách Đảng ủy Nguyễn Quang Thái: https://ttmailuongkhoi.moj.gov.vn | | |
| | Trang tin thứ trưởng T.T Nguyễn Thanh Ngọc: https://ttnguyenthanhngoc.moj.gov.vn | | |
| | Trang tin Phó Bí thư chuyên trách Đảng ủy Nguyễn Quang Thái: https://ttnguyenquangthai.moj.gov.vn | | |
| | Trang tin thứ trưởng T.T Nguyễn Thanh Tú: https://ttnguyenthanhtu.moj.gov.vn | | |
| | Trang thông tin Trợ giúp pháp lý: https://tgpl.moj.gov.vn | | |
| | Trang thông tin Chuyển đổi số: https://dx.moj.gov.vn | | |
| **2** | **Hệ thống thông tin báo cáo:** https://baocao.moj.gov.vn | Ứng dụng | 1 |
| **3** | **Hệ thống quản lý đầu tư công Bộ Tư pháp** https://quanlyduan.moj.gov.vn | Ứng dụng | 1 |
| **4** | **Phần mềm Hệ thống quản lý văn bản và điều hành tác nghiệp:** https://vbdh.moj.gov.vn | Ứng dụng | 1 |
| **II** | **HỆ THỐNG MÁY CHỦ** | | |
| **1** | Máy chủ ảo hóa | Máy chủ | 26 |

*3.2. Yêu cầu kỹ thuật chi tiết:*

*a) Yêu cầu về chất lượng kiểm tra, đánh giá an toàn thông tin cho hệ thống thông tin, phần mềm*

- Việc kiểm tra, đánh giá phải tuân thủ theo các tiêu chuẩn quốc tế như OWASP, OSSTMM…

- Việc kiểm tra đánh giá cần sử dụng các công cụ chuyên dụng như BurpSuite, Acunetix, ZAP… hoặc sử dụng công cụ đánh giá tự phát triển.

- Việc kiểm tra đánh giá an toàn cho hệ thống thông tin cần bao gồm nhưng không giới hạn các hạng mục sau:

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| 1 | Thu thập thông tin | Thu thập / thăm dò thông tin về việc rò rỉ dữ liệu qua các công cụ tìm kiếm |
| | | Lấy thông tin máy chủ Web |
| | | Mô hình hóa kiến trúc của các ứng dụng |
| | | Xem xét Metafiles của máy chủ về việc rò rỉ thông tin |
| | | Liệt kê phần mềm trên máy chủ |
| | | Xem xét Comments và Metadata của máy chủ về việc rò rỉ thông tin |
| | | Xác định các điểm đầu vào của phần mềm |
| | | Tìm kiếm các khả năng thực thi qua ứng dụng |
| | | Kiểm tra Web Application Framework |
| | | Kiểm tra ứng dụng Web |
| 2 | Kiểm tra quản lý cấu hình và triển khai | Kiểm tra cấu hình mạng / cơ sở hạ tầng |
| | | Kiểm tra cấu hình nền tảng ứng dụng |
| | | Kiểm tra việc xử lý phần mở rộng tệp cho thông tin nhạy cảm |
| | | Xem lại các tệp cũ, sao lưu và không được tham chiếu để biết thông tin nhạy cảm |
| | | Liệt kê cơ sở hạ tầng và giao diện quản trị ứng dụng |
| | | Kiểm tra các phương pháp HTTP |
| | | Kiểm tra chính sách tên miền chéo RIA |
| | | Kiểm tra bảo mật truyền tải nghiêm ngặt HTTP |
| 3 | Kiểm tra quản lý danh tính | Định nghĩa vai trò thử nghiệm |
| | | Kiểm tra quy trình đăng ký người dùng |
| | | Kiểm tra quy trình cấp phép tài khoản |
| | | Kiểm tra để liệt kê tài khoản và tài khoản người dùng có thể đoán được |
| | | Kiểm tra chính sách tên người dùng yếu hoặc không được thực thi |
| 4 | Kiểm tra xác thực | Kiểm tra thông tin xác thực được truyền qua kênh được mã hóa |

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| | | Kiểm tra thông tin đăng nhập mặc định |
| | | Kiểm tra cơ chế khóa yếu |
| | | Kiểm tra để bỏ qua lược đồ xác thực |
| | | Kiểm tra chức năng ghi nhớ mật khẩu |
| | | Kiểm tra điểm yếu của bộ đệm trình duyệt |
| | | Kiểm tra chính sách mật khẩu yếu |
| | | Kiểm tra câu hỏi / câu trả lời bảo mật yếu |
| | | Kiểm tra các chức năng thay đổi hoặc đặt lại mật khẩu yếu |
| | | Kiểm tra xác thực yếu hơn trong kênh thay thế |
| 5 | Kiểm tra ủy quyền | Kiểm tra truyền tải thư mục / tệp bao gồm |
| | | Kiểm tra để bỏ qua giản đồ ủy quyền |
| | | Kiểm tra để nâng cấp đặc quyền |
| | | Kiểm tra các tham chiếu đối tượng trực tiếp không an toàn |
| 6 | Kiểm tra quản lý phiên | Thử nghiệm để bỏ qua cơ chế quản lý phiên |
| | | Kiểm tra các thuộc tính Cookies |
| | | Kiểm tra sự cố định phiên |
| | | Kiểm tra các biến phiên tiếp xúc |
| | | Kiểm tra truy vấn yêu cầu trên nhiều trang web (CSRF) |
| | | Kiểm tra chức năng đăng xuất |
| | | Kiểm tra thời gian chờ phiên |
| | | Kiểm tra phiên |
| 7 | Kiểm tra xác thực đầu vào | Thử nghiệm Reflected Cross Site Scripting |
| | | Thử nghiệm Stored Cross Site Scripting |
| | | Kiểm tra giả mạo các phương HTTP |
| | | Kiểm tra Thông số HTTP Pollution |
| | | Kiểm tra SQL Injection |
| | | Kiểm tra ORM Injection |
| | | Kiểm tra XML Injection |
| | | Kiểm tra SSI Injection |

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| | | Thử nghiệm cho XPath Injection |
| | | Thử nghiệm Code-Injection |
| 8 | Kiểm tra để xử lý lỗi | Phân tích Error Codes |
| | | Phân tích Stack Traces |
| 9 | Kiểm tra mật mã yếu | Kiểm tra mật mã SSL / TLS yếu, bảo vệ lớp truyền tải không đủ |
| | | Kiểm tra thông tin nhạy cảm được gửi qua các kênh không được mã hóa |
| | | Kiểm tra Padding Oracle |
| 10 | Kiểm tra Logic | Kiểm tra xác thực dữ liệu logic |
| | | Kiểm tra khả năng giả mạo yêu cầu |
| | | Kiểm tra tính toàn vẹn |
| | | Kiểm tra thời gian quy trình |
| | | Số lần kiểm tra một chức năng có thể được sử dụng giới hạn |
| | | Kiểm tra việc phá vỡ quy trình làm việc |
| | | Kiểm tra các biện pháp bảo vệ chống lại việc lạm dụng ứng dụng |
| | | Kiểm tra tải lên các loại tệp không mong muốn |
| | | Kiểm tra tải lên các tệp độc hại |
| 11 | Kiểm tra phía Client-Side | Thử nghiệm cho Kịch bản chéo trang dựa trên DOM |
| | | Kiểm tra thực thi JavaScript |
| | | Kiểm tra HTML Injection |
| | | Kiểm tra chuyển hướng URL phía máy khách |
| | | Kiểm tra để đưa vào CSS |
| | | Kiểm tra thao tác tài nguyên phía máy khách |
| | | Thử nghiệm Cross-Origin Resource Sharing |
| | | Thử nghiệm nhấp nháy Cross-Site Flashing |
| | | Kiểm tra Clickjacking |
| | | Kiểm tra Web Socket |
| | | Kiểm tra Web Mesages |
| | | Kiểm tra bộ nhớ cục bộ |

*b) Yêu cầu về chất lượng dịch vụ kiểm tra, đánh giá an toàn thông tin hệ thống máy chủ tại Trung tâm dữ liệu điện tử Bộ Tư pháp*

- Việc kiểm tra đánh giá cần sử dụng các công cụ chuyên dụng như Nessus, Rapid 7, Nmap … hoặc sử dụng công cụ đánh giá tự phát triển.

- Việc thực hiện kiểm tra đánh giá an toàn cho máy chủ cần bao gồm nhưng không giới hạn các hạng mục sau:

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| 1 | Khảo sát thu thập thông tin | Thu thập toàn bộ các thông tin liên quan đến mạng, hệ điều hành và các ứng dụng |
| | | Thông tin về các thiết bị mạng như địa chỉ IP, hãng sản xuất, phiên bản firmware, OS... |
| | | Thông tin về mô hình mạng, vị trí cài đặt và chức năng của từng thiết bị. |
| | | Thông tin về các máy chủ như địa chỉ IP, hệ điều hành, mục đích, chức năng của các máy chủ. |
| | | Thông tin về các cổng mở, dịch vụ đang chạy trên máy chủ, phần mềm và phiên bản của các dịch vụ và các thông tin khác. |
| 2 | Kiểm tra các dịch vụ | Fingerprint Server |
| | | Performing vulnerability scanning |
| | | Kiểm tra quyền Dịch vụ đang chạy |
| | | Kiểm tra NetBIOS và SMB |
| | | Cài đặt cho đăng nhập từ xa |
| | | DNSrecon |
| | | Brute Force SSH, FTP và thông tin đăng nhập các dịch vụ khác |
| | | Kiểm tra các dịch vụ không an toàn: FTP, SMTP và NNTP |
| | | Kiểm tra tài khoản khách, tài khoản mặc định hoặc không sử dụng |
| | | Kiểm tra tài nguyên mặc định hoặc ứng dụng mẫu |
| | | Liệt kê các thư mục máy chủ web |
| | | Kiểm tra xem các dịch vụ không cần thiết có bị tắt / đóng hay không. |
| | | Kiểm tra WebDAV |

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| | | Kiểm tra quyền truy cập ẩn danh |
| 3 | Kiểm tra cấu hình và kiểm thử máy chủ ứng dụng | Kiểm tra OpenSSL Heartbleed |
| | | Kiểm tra Web Cache Deception |
| | | Kiểm tra Basic Authorization over HTTP |
| | | Kiểm tra Insecure Transportation Security Protocol Supported (SSLv2) |
| | | Kiểm tra ROBOT Attack Detected (Weak Oracle) |
| | | Kiểm tra SVN |
| | | Kiểm tra Unrestricted File Upload |
| | | Kiểm tra Code Execution via WebDAV |
| | | Kiểm tra Apache Server-Info |
| | | Gửi biểu mẫu quan trọng tới HTTP |
| | | Sử dụng HTTP không an toàn |
| | | Kiểm tra Open Policy Crossdomain.xml |
| | | Kiểm tra SQLite Database |
| | | Kiểm tra Sublime SFTP Config File |
| | | Kiểm tra Backup File |
| | | Kiểm tra Database Error Message |
| | | Kiểm tra Insecure Transportation Security Protocol Supported (TLS 1.0) |
| | | Kiểm tra Misconfigured Access-Control-Allow-Origin Header |
| | | Kiểm tra Programming Error Message |
| | | Kiểm tra Version Disclosure |
| | | Kiểm tra Windows Username Disclosure |
| | | Kiểm tra Bash Command Injection Vulnerability (Shellshock Bug) |
| | | Khai thác các mã CVE đã được công khai |
| | | Kiểm tra Elmah.axd / Errorlog.axd |
| | | Password được truyền qua giao thức HTTP |
| | | Kiểm tra CVS |
| | | Kiểm tra Weak Basic Authentication Credentials |

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| | | Kiểm tra Active Mixed Content over HTTPS |
| | | Kiểm tra Apache Server-Status |
| | | Kiểm tra Critical Form Served over HTTP |
| | | Kiểm tra Insecure Transportation Security Protocol Supported (SSLv3) |
| | | Kiểm tra RSA Private Key Detected |
| | | Kiểm tra SSL/TLS Not Implemented |
| | | Kiểm tra Unicode Transformation (Best-Fit Mapping) |
| | | Kiểm tra Debug Mode Enabled |
| | | Kiểm tra Database Name Disclosure |
| | | Kiểm tra Internal IP Address Disclosure |
| | | Kiểm tra Misconfigured Frame |
| | | Kiểm tra Stack Trace Disclosure |
| | | Kiểm tra ViewState không được mã hóa |
| | | Liệt kê cơ sở hạ tầng và giao diện quản trị ứng dụng |
| | | Kiểm tra Web Backdoor |
| | | Kiểm tra Backup Source Code |
| | | Kiểm tra Expression Language Injection |
| | | Kiểm tra ROBOT Attack Detected (Strong Oracle) |
| | | Kiểm tra GIT |
| | | Kiểm tra Trace.axd |
| | | Kiểm tra WebDAV Directory |
| | | Kiểm tra HTTP Header Injection |
| | | Kiểm tra Invalid SSL Certificate |
| | | Kiểm tra Source Code Disclosure |
| | | Kiểm tra Stack Trace Disclosure |
| | | Kiểm tra Weak Ciphers Enabled |
| | | Kiểm tra DS_Store File Found |
| | | Kiểm tra Log File |
| | | Kiểm tra Misconfigured X-Frame-Options Header |
| | | Kiểm tra TRACE/TRACK Method |

| Stt | Hạng mục | Nội dung thực hiện |
|---|---|---|
| | | Kiểm tra Windows Short Filename |
| 4 | Thử nghiệm xâm nhập | Loại bỏ những kết quả sai mà công cụ dò quét được. |
| | | Minh họa cách thức khai thác điểm yếu, giúp khách hàng hiểu rõ mức độ nguy hiểm và ảnh hưởng của điểm yếu đối với hệ thống mạng |
| | | Password attack: Thử nghiệm các kiểu tấn công password vào các thiết bị mạng, bảo mật và thiết bị truyền dẫn |
| | | Exploits: Thử nghiệm khai thác các lỗ hổng bảo mật được tìm thấy ở phần trước. |

*c) Yêu cầu dịch vụ hỗ trợ kỹ thuật, bảo hành, bảo dưỡng*

- Cam kết về thời gian tiếp nhận thông tin thông báo sự cố: 24 giờ/ngày, 7 ngày/tuần (kể cả ngày nghỉ và ngày lễ).

- Cam kết có kỹ thuật viên hỗ trợ xử lý kỹ thuật, ứng cứu sự cố: Nhà cung cấp dịch vụ sẽ có mặt trong vòng 2 giờ kể từ khi nhận được thông báo của Chủ đầu tư (qua điện thoại, email...) để thực hiện xử lý, khắc phục sự cố. Việc hỗ trợ kỹ thuật được thực hiện tại Bộ Tư pháp, 60 Trần Phú, phường Ba Đình, thành phố Hà Nội.

**4. Giải pháp và phương pháp luận:**

*Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:*

*1. Giải pháp và phương pháp luận;*

Giải pháp và phương pháp luận cho việc triển khai cung cấp dịch phải phù hợp với các yêu cầu được nêu tại Mục 2, Chương V (nêu trên).

*2. Kế hoạch công tác.*

Thể hiện quy trình triển khai công việc hợp lý, khả thi và phân công nhân sự đề xuất phù hợp với tiến trình công việc

**5. Quy định về kiểm tra, nghiệm thu sản phẩm:**

Sau khi kiểm tra sản phẩm dịch vụ đáp ứng các yêu cầu kỹ thuật quy định tại Chương V, Chủ đầu tư, nhà thầu và các bên có liên quan sẽ tiến hành nghiệm thu sản phẩm dịch vụ để đưa vào sử dụng.

Các quy định khác về kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm để phục vụ công tác thanh, quyết toán hợp đồng thực hiện theo các quy định của pháp luật hiện hành và nội dung công việc của gói thầu