NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Số: 878 /TTTD-QLĐT
V/v mời báo giá dịch vụ nâng cấp hệ thống Cổng thông tin KHV M5

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 26 tháng 5 năm 2026

Kính gửi:

Trung tâm Thông tin tín dụng Quốc gia Việt Nam (CIC) có kế hoạch Nâng cấp hệ thống Cổng thông tin Khách hàng vay M5. CIC mời Quý đơn vị cung cấp báo giá đối với các hàng hóa, dịch vụ gửi kèm công văn này.

Đề nghị Quý đơn vị gửi báo giá về Trung tâm Thông tin tín dụng Quốc gia Việt Nam (Địa chỉ: số 45 Lý Thường Kiệt, phường Cửa Nam, thành phố Hà Nội) đồng thời gửi bản mềm về địa chỉ email: qldt@creditinfo.org.vn, phongketoan@creditinfo.org.vn. Báo giá của Quý đơn vị là cơ sở để CIC xây dựng dự toán và thực hiện thủ tục mua sắm theo quy định hiện hành.

Thời hạn gửi báo giá: chậm nhất ngày 02/6/2026. Báo giá có hiệu lực tối thiểu 60 ngày.

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- P. NCPT, P. TCKT (Để đăng tải);
- Lưu VT, QLĐT.LTNhung.

Gửi kèm:
- Yêu cầu kỹ thuật.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Lê Anh Tuấn

Tài liệu YCKT: Nâng cấp hệ thống Cổng thông tin khách hàng vay M5

(Đính kèm công văn số: ..878..../TTTD - QLĐT ngày 26/5/2026)

I. THÔNG TIN CHUNG

1.1. Mục đích tài liệu

Tài liệu này xác định toàn bộ yêu cầu kỹ thuật cho dự án nâng cấp hệ thống M5 của Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC). Tài liệu là cơ sở pháp lý và kỹ thuật để các bên liên quan thống nhất phạm vi công việc, tiêu chí nghiệm thu và trách nhiệm thực hiện.

1.2. Phạm vi áp dụng

Tài liệu áp dụng cho toàn bộ các hạng mục kỹ thuật của dự án, bao gồm:

- Nâng cấp hạ tầng hệ điều hành từ CentOS 6 / Oracle Linux 6 lên RHEL 9
- Hiện đại hóa kiến trúc ứng dụng: loại bỏ WebLogic, chuyển sang Spring Boot + Embedded Tomcat
- Nâng cấp runtime: Java 8 → Java 21, Spring Boot 2.0.5 → 3.x
- Nâng cấp frontend: Angular 6 → Angular 19
- Thay thế và làm sạch toàn bộ thư viện EOL/CVE (frontend & backend)
- Triển khai HashiCorp Vault – quản lý secrets tập trung
- Thiết lập hệ thống giám sát, logging và observability
- Xử lý các điểm yếu bảo mật có thể khai thác trực tiếp

II. BỐI CẢNH VÀ LÝ DO NÂNG CẤP

2.1. Hiện trạng hệ thống

Hệ thống M5 hiện đang vận hành trên nền tảng hạ tầng và phần mềm đã hết vòng đời hỗ trợ (End-of-Life).

Thành phần	Phiên bản hiện tại	Trạng thái	Rủi ro chính
Hệ điều hành	CentOS 6 / OL 6	**EOL**	Không có bản vá Kernel, sudo, polkit; leo thang đặc quyền
Middleware	WebLogic 12c	**Rủi ro cao**	Nhiều lỗ hổng RCE; khó vá triệt để (CVE-2019-2729, CVE-2020-2555)
Runtime	Java 8	**EOL**	Không tương thích stack mới; giảm khả năng nhận bản vá
Framework BE	Spring Boot 2.0.5	**EOL**	Khó duy trì, khó vá, khó tương thích hệ sinh thái mới

Framework FE	Angular 6.1.0	**EOL**	60+ CVEs; toàn bộ chuỗi phụ thuộc frontend bị ảnh hưởng
Secrets/Config	JNDI tĩnh	**Không an toàn**	Khó xoay vòng mật khẩu; rủi ro lộ thông tin kết nối

2.2. Mục tiêu dự án

- Loại bỏ hoàn toàn các nền tảng EOL, giải quyết triệt để các lỗ hổng bảo mật
- Đảm bảo Zero Downtime trong quá trình chuyển đổi
- Tuân thủ đầy đủ quy định của Nhà nước về an toàn, an ninh thông tin
- Tạo nền tảng kỹ thuật bền vững, sẵn sàng mở rộng trong 5–10 năm tới
- Tối ưu chi phí TCO (Total Cost of Ownership) dài hạn

III. YÊU CẦU KỸ THUẬT – HẠ TẦNG & MÔI TRƯỜNG

3.1. Yêu cầu hệ điều hành

Toàn bộ 11 máy chủ ảo hóa phải được cài đặt Red Hat Enterprise Linux 9 (RHEL 9) bản mới nhất tại thời điểm triển khai.

Tiêu chí	Yêu cầu
Phiên bản OS	Red Hat Enterprise Linux 9.x (LTS)
Kiến trúc	x86_64
Subscription	Red Hat Subscription hợp lệ, đăng ký với Red Hat Customer Portal
SELinux	Bật chế độ Enforcing; cấu hình policy phù hợp với ứng dụng
Firewall	firewalld bật; chỉ mở port theo danh sách được phê duyệt
SSH	Xác thực bằng SSH Key; tắt đăng nhập root qua SSH; đổi port mặc định
NTP / Timezone	Đồng bộ NTP với máy chủ nội bộ; Timezone: Asia/Ho_Chi_Minh
Audit Logging	auditd bật; log lưu tối thiểu 90 ngày
Cập nhật bản vá	Áp dụng tất cả bản vá bảo mật RHEL 9 trước ngày Go-live

3.2. Phân bố và cấu hình 11 máy chủ

Hệ thống sử dụng 11 máy chủ ảo hóa (VM) được phân bổ theo chức năng như sau:

STT	Nhóm	Hostname	Cấu hình	Chức năng
1	Web App	**WEBAPP-01**	8C/16GB/150GB	Web M5 (Primary), mount NFS
2	Web App	**WEBAPP-02**	8C/16GB/150GB	Web M5 (Load Balancing)
3	Mobile	**MOBILE-API-01**	8C/16GB/150GB	API Gateway cho Mobile App
4	Mobile	**MOBILE-API-02**	8C/16GB/150GB	API Gateway dự phòng
5	Service	**SERVICE-01**	8C/16GB/150GB	Tích hợp CIC, Admin Portal
6	Service	**SERVICE-02**	8C/16GB/150GB	Backup cho SERVICE-01
7	Middle ware	**QUEUE-CACHE-01**	8C/16GB/150GB	RabbitMQ, Redis, SMS/Mail
8	Middle ware	**QUEUE-CACHE-02**	8C/16GB/150GB	RabbitMQ, Redis, SMS/Mail
9	Middle ware	**QUEUE-CACHE-03**	8C/16GB/150GB	RabbitMQ, Redis, SMS/Mail
10	DMZ	**DMZ-01**	8C/16GB/150GB	Proxy Server, Internet
11	DMZ	**DMZ-02**	8C/16GB/150GB	Proxy Server dự phòng (HA)

3.3. Yêu cầu lưu trữ và mạng

- NFS Shared Storage: mount trên 9 server ứng dụng (WEBAPP, MOBILE-API, SERVICE, QUEUE-CACHE); dung lượng tối thiểu 1TB; hỗ trợ đồng bộ file tĩnh
- Network: VLAN tách biệt cho DMZ và Internal App; băng thông tối thiểu 1Gbps giữa các VM
- Load Balancer: cấu hình điều hướng lưu lượng cho cặp WEBAPP-01/02 và MOBILE-API-01/02
- Firewall Rules: chỉ mở port 80/443 ra Internet qua DMZ; các port nội bộ theo ma trận kết nối được phê duyệt

3.4. Yêu cầu Runtime

Thành phần	Phiên bản hiện tại	Phiên bản yêu cầu	Ghi chú

JDK	Java 8	**Java 21 (LTS)**	Cài bản build tương thích RHEL 9; giai đoạn đầu có thể dùng Java 8 mới nhất
Application Server	WebLogic 12c	**Embedded Tomcat**	Loại bỏ hoàn toàn phụ thuộc WebLogic
systemd	Không có	**Bắt buộc**	Viết unit file quản lý Start/Stop/Restart/Status cho từng service

IV. YÊU CẦU KỸ THUẬT – ỨNG DỤNG

4.1. Kiến trúc mục tiêu

- Mỗi ứng dụng đóng gói thành file JAR/WAR độc lập, vận hành theo mô hình Spring Boot Standalone
- Loại bỏ toàn bộ phụ thuộc WebLogic khỏi pom.xml và mã nguồn
- Cấu hình và secrets lấy động từ HashiCorp Vault Agent (không dùng file config tĩnh)
- File tĩnh (ảnh, tài liệu) ghi vào đường dẫn NFS Shared Storage, không ghi local disk

4.2. Nâng cấp Backend

Hạng mục	Từ	Đến	Yêu cầu bổ sung
Spring Boot	2.0.5	**3.x (LTS)**	Migration toàn bộ Jakarta EE namespace; kiểm tra SecurityConfig
Java	8	**21 (LTS)**	Bật Virtual Threads nếu phù hợp; tối ưu JVM flags cho G1GC
bouncycastle	1.38	**1.78+**	Thư viện mật mã lõi – nâng ngay trong sprint đầu
jjwt	0.10.5	**0.12.x**	Liên quan xử lý JWT; kiểm tra lại claim parsing sau nâng cấp
jsoup	1.11.3	**1.17.x**	Vá XXE/CVE; kiểm tra lại các đoạn parse HTML
iText PDF	2.1.7 / 5.5.13	**iText 7.x**	Kiểm tra license; tương thích xử lý font tiếng Việt
groovy-all	2.4.5	**Nâng hoặc loại bỏ**	Đánh giá sự phụ thuộc; ưu tiên loại bỏ nếu không cần thiết

commons-imaging	1.0-alpha3	**Stable release**	Thay bản stable; không dùng bản alpha trong môi trường production
firebaseadmin	8.1.0	**Bản mới nhất**	Cập nhật SDK; kiểm tra breaking changes với push notification
okhttp	4.9.1	**Bản mới nhất**	Kiểm tra compatibility với HTTP/2 và TLS settings

4.3. Nâng cấp Frontend

Thư viện	Từ	Đến	Yêu cầu bổ sung
@angular/core	6.1.0	**Angular 19**	Nâng theo lộ trình trung gian (12→15→17→19); kiểm tra từng bước
TypeScript	2.7.2	**5.x**	Tương thích Angular 19; cập nhật tsconfig.json
RxJS	6.1.0	**7.8.x**	Kiểm tra deprecated operator; thay thế pipe patterns
webpack	4.8.0	**5.x hoặc Vite**	Angular 19 mặc định dùng esbuild; xem xét loại bỏ webpack custom
core-js	2.5.7	**3.x**	Polyfill mới; không còn unmaintained
Bootstrap	4.6.2	**5.x**	Loại bỏ jQuery dependency; cập nhật class names theo Bootstrap 5
moment.js	2.22.2	**date-fns hoặc Day.js**	moment.js đã deprecated; chuyển sang thư viện nhẹ hơn, tree-shakeable
tslint	5.9.1	**ESLint + @angular-eslint**	tslint deprecated; chuyển toàn bộ rules sang ESLint config
codelyzer	4.2.1	**@angular-eslint**	Thay thế bằng @angular-eslint/eslint-plugin-template
zone.js	0.8.26	**Theo Angular 19**	Angular 19 hỗ trợ Zoneless; đánh giá nhu cầu trước khi loại bỏ

4.4. Danh sách ứng dụng trong phạm vi

STT	Tên ứng dụng	Chức năng	Server triển khai
1	**Web M5**	Ứng dụng web dành cho khách hàng vãng lai (KHV)	WEBAPP-01, WEBAPP-02
2	**Mobile API**	API Gateway cung cấp dịch vụ cho Mobile App	MOBILE-API-01, MOBILE-API-02
3	**Admin Portal**	Giao diện quản trị hệ thống	SERVICE-01
4	**Service CIC**	Tích hợp lấy thông tin khách hàng từ kho CIC	SERVICE-01, SERVICE-02
5	**SMS/Mail Service**	Dịch vụ gửi email và SMS thông báo	QUEUE-CACHE-01, QUEUE-CACHE-02
6	**DMZ Proxy**	Proxy điều hướng lưu lượng Internet	DMZ-01, DMZ-02

V. YÊU CẦU KỸ THUẬT – BẢO MẬT

5.1. HashiCorp Vault – Quản lý Secrets

Yêu cầu	Chi tiết
Vault Agent	Cài đặt Vault Agent trên tất cả 11 VM; auto-auth với AppRole
Database Credentials	Ứng dụng fetch credentials từ Vault khi khởi động; không lưu trong file config hay JNDI
Secret Rotation	Hỗ trợ xoay vòng mật khẩu DB tự động mà không restart ứng dụng
JWT / Token Secret	JWT signing key lưu trong Vault; loại bỏ toàn bộ hardcode trong mã nguồn
Audit Log	Bật Vault Audit Device; log mọi truy cập secret; lưu tối thiểu 90 ngày
High Availability	Vault triển khai HA (tối thiểu 3 node) hoặc kết nối với Vault Enterprise của đơn vị

5.2. Yêu cầu Hardening hệ điều hành

- Tắt tất cả dịch vụ không cần thiết (telnet, rsh, rlogin, ftp)
- Cấu hình password policy: độ dài tối thiểu 12 ký tự, lịch sử 12 mật khẩu
- Giới hạn su/sudo theo nhóm người dùng được phê duyệt

- Cấu hình sysctl: kernel.dmesg_restrict, net.ipv4.conf.all.rp_filter, kernel.randomize_va_space
- Scan lỗ hổng bằng OpenSCAP/Lynis trước Go-live; tất cả CRITICAL phải được vá

VI. YÊU CẦU GIÁM SÁT, LOGGING VÀ OBSERVABILITY

6.1. Monitoring Stack

Thành phần	Server	Yêu cầu
Grafana	GRAFANA	Dashboard CPU, RAM, Disk, Network cho tất cả 11 VM; alert khi ngưỡng > 80%
Prometheus	GRAFANA	Scrape metrics 15s/lần; retention 30 ngày; cấu hình alerting rules
Node Exporter	11 VM	Cài đặt trên toàn bộ 11 server; expose metrics qua port được phê duyệt
ELK Stack	ELK-APM	Elasticsearch + Logstash + Kibana; index log theo ngày; retention 90 ngày
Filebeat	11 VM	Đẩy application log và system log về ELK; format JSON chuẩn; không mất log khi restart
APM Agent	App Servers	Elastic APM tích hợp trong ứng dụng Spring Boot; trace request end-to-end

6.2. Yêu cầu Health Check

- Mỗi ứng dụng Spring Boot phải expose endpoint /actuator/health trả về trạng thái UP/DOWN
- Health check kiểm tra: kết nối Database, kết nối Vault, kết nối RabbitMQ/Redis
- Grafana alert gửi thông báo (email/webhook) khi service DOWN

6.3. Log Standards

- Format log: JSON có các trường bắt buộc: timestamp, level, service, traceId, message
- Log level: ERROR cho exception, WARN cho cảnh báo nghiệp vụ, INFO cho sự kiện quan trọng
- Không ghi thông tin nhạy cảm (password, token, CMND, số tài khoản) vào log
- Log rotation: hàng ngày; nén sau 7 ngày; xóa sau 90 ngày trên local; đẩy ELK giữ 90 ngày

VII. Lộ trình triển khai 03 tháng (12 tuần)

7.1 Lộ trình triển khai

Lộ trình triển khai được tổ chức theo nguyên tắc song song ngay từ đầu dự án. Nhóm hạ tầng thực hiện dựng mới môi trường RHEL 9, chuẩn hóa bảo mật, giám sát và

secrets; trong khi đó nhóm ứng dụng đồng thời refactor mã nguồn, loại bỏ phụ thuộc WebLogic, nâng cấp backend/frontend và xử lý các điểm yếu bảo mật trong code. Hai nhánh chỉ hội tụ tại các mốc kiểm thử tích hợp, triển khai thử nghiệm, parallel run và cutover.

Tuần	Đầu việc trọng tâm	Kết quả kỳ vọng	Phụ thuộc
Tuần 1-2	(1) Hạ tầng: khởi tạo 11 VM RHEL 9; cấu hình network, firewall, storage, policy, JDK. (2) Phần mềm: rà soát mã nguồn, chốt danh mục dependency EOL/CVE, thiết kế refactor và kế hoạch nâng cấp backend/frontend.	Môi trường đích được dựng song song với việc hoàn tất thiết kế nâng cấp phần mềm	Danh sách máy chủ, policy và phạm vi mã nguồn được chốt
Tuần 3-4	(1) Hạ tầng: triển khai Grafana, Prometheus, ELK/APM, Filebeat, Vault Agent, hardening. (2) Phần mềm: tách phụ thuộc WebLogic, chuẩn hóa cấu hình, xử lý hardcode secrets, token, RBAC, SSL/TLS, upload.	Hạ tầng có giám sát và secrets; mã nguồn hoàn tất refactor nền để build theo mô hình mới	Kết quả khảo sát tuần 1-2
Tuần 5-6	(1) Hạ tầng: hoàn thiện Redis, RabbitMQ, NFS, systemd, CI/CD, observability. (2) Phần mềm: nâng backend Java 8 -> Java 21, Spring Boot 2 -> 3, cập nhật thư viện backend trọng yếu, build và sửa lỗi tương thích.	Nền tảng vận hành sẵn sàng; backend chạy được trên stack mới	Refactor nền và môi trường đích đã sẵn sàng
Tuần 7-8	(1) Hạ tầng: tinh chỉnh hiệu năng, bảo mật nền tảng, kiểm tra HA/backup/logging. (2) Phần mềm: nâng frontend Angular theo lộ trình trung gian -> mục tiêu, cập nhật toolchain và thư viện frontend, chỉnh UI/API tương thích.	Frontend và backend cùng đạt trạng thái sẵn sàng kiểm thử tích hợp	Backend đã ổn định; nền tảng observability đã chạy
Tuần 9-10	Triển khai gói phần mềm nâng cấp lên môi trường RHEL 9; kiểm thử tích hợp end-to-end, UAT nội bộ, stress test, security test, rà	Có bản triển khai tích hợp hoàn chỉnh trên môi trường mới	Hai nhánh hạ tầng và phần mềm đều hoàn thành mốc kỹ thuật chính

	soát checklist go-live.		
Tuần 11	Parallel run giữa hệ thống cũ và mới; đồng bộ dữ liệu/file, so sánh kết quả xử lý, diễn tập rollback, chốt cấu hình vận hành.	Xác nhận hệ thống mới đáp ứng yêu cầu vận hành thực tế	Kết quả kiểm thử tuần 9-10 đạt yêu cầu
Tuần 12	Cutover qua Load Balancer, smoke test, theo dõi hậu kiểm, tối ưu sau go-live và bàn giao vận hành.	Hệ thống mới vận hành chính thức, ổn định và có phương án theo dõi sau triển khai	Parallel run thành công

7.2 Cam kết cấp hệ thống và bảo hành

- Tuân thủ quy định an toàn bảo mật cấp độ 3 đối với phần mềm và máy chủ (OS).
- Mã nguồn phải được rà soát lỗ hổng bảo mật
- Thời gian bảo hành: 01 năm kể từ ngày nghiệm thu.