Testing & Evaluation Sheet	
Proton VPN	
1. Tool Overview	
Name:	Proton VPN
Category:	VPN (Virtual Private Network)
Purpose:	Proton VPN provides secure and private internet browsing by encrypting user traffic and masking their IP address, offering enhanced online privacy and anonymity.
Date Tested	4/15/25
Status:	Deployed ☑ Operational - Actively running/maintained ☐ In Testing - Currently being evaluated or piloted ☐ Inactive/Deprecated - No longer maintained or functional
Deployment Architecture:	☐ A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server) ☐ A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud) ☑ A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.) ☐ A service that is hosted by a third party but can also be self-hosted
Version:	ProtonVPN v4.0
2. Installation & Setup	
OS Compatibility	Windows, macOS, iOS, Linux, Android
Installation Manual:	Yes – Available through ProtonVPN Support and GitHub README files for open-source repositories.
Installation Steps:	1. Go to the Official Website - Open your browser and go to https://protonvpn.com/download

	2. Download the App - Download the correct installer for your device from the ProtonVPN download page - Open the downloaded .dmg file and drag the app into Applications 3. Install the App - Open the .dmg file. - Drag the ProtonVPN icon into the Applications folder. 4. Launch the App - Open ProtonVPN from your Applications folder (or Spotlight). 5. Sign In - Enter your Proton account credentials (you can create an account on their website if you don't have one). 6. Connect to a Server - Click "Quick Connect" for the fastest connection. - Or choose a country/server manually. 7. Done! - You're now securely connected to the internet via ProtonVPN.
Mention if command-line setup or special configurations are needed	- Developer Build (macOS/iOS): - Requires intermediate to advanced experience with Xcode and Swift. Manual setup includes dependency installation, credentials configuration, and code signing. - End Users (Windows/macOS/Linux): - No command-line setup or special configuration needed. GUI-based installers handle all dependencies and configurations automatically. - Everyday Users: - No technical knowledge required. Simply install the app and log in.
Common Installation Issues & Fixes:	1. Error: "Failed to resolve dependencies with Swift Package Manager" (macOS/iOS) a. Fix: Ensure that your internet connection is stable and that Xcode is properly configured. Run xcode-select --install to update Xcode's command-line tools. 2. Error: "Code signing required for VPN entitlements" (macOS/iOS) a. Fix: Ensure you are using a paid Apple Developer account and that your bundle identifier is unique in Xcode. 3. Error: "OpenVPN configuration file missing" (Windows)

	a. Fix: Ensure that the OpenVPN file exists in the default directory. Reinstall Proton VPN if the file is missing. 4. Error: “TAP adapter not installed” (Windows) a. Fix: Make sure that the TAP adapter installation process completes. Try reinstalling Proton VPN to resolve the issue. 5. Error: “TLS certificate pinning disabled” (Windows) a. Fix: To monitor HTTP traffic, provide an empty “TlsPinningConfig” value in the configuration file: "TlsPinningConfig": {}
User Documentation:	Yes - Official documentation on ProtonVPN’s website - GitHub repos have developer-specific README and integration notes
Required Technical Knowledge	- End User: Beginner (GUI-based, no CLI required for most installs) - Developer Build: Intermediate to Professional (especially on iOS/macOS builds from source)

3. Testing & Evaluation

Category	Details	Score
Operational Functionality:	**Functionality** ● Test Steps: Verify the tool’s core features by using all major functions, tracking any failures or bugs. ☐ The tool is mostly non-functional with many broken features and bugs. ☐ Several broken features or bugs ☐ Minor bugs or issues ☐ Mostly functional with few bugs or no bugs ☑ Fully functional with no bugs **Internet Dependence:** ● No offline functionality; requires an active internet connection. ● Performs fine on 2G/3G networks, but speeds may be limited. **Localization & Language Support** ● Supports over 20 languages, including English, Spanish, French, German, Japanese, and more.	4

	● The Proton community translation program invites users to help translate Proton products (including ProtonVPN) into multiple languages. They use platforms like Crowdin to manage and coordinate community-driven localization efforts. ● However, not really much localization for East Asian Languages **Mobile Accessibility** ● Very mobile-friendly; dedicated apps for iOS and Android with a clean, responsive UI.	
Usability for Non-Technical Users	**Ease of Installation & Deployment** ● Easy; apps available on app stores and official sites. No command-line use required for regular users ● Setup guides, manuals and FAQ's are well-maintained and accessible on the ProtonVPN support site ● Typical installation takes 3-5 minutes **User Onboarding Experience** ● Includes onboarding prompts, FAQs, and tutorials **Technical Experience Level Required** ● For End Users, tool is easy to use and install and UI is non-technical friendly with a modern layout and clearly labeled features.	4.3
Security & Privacy Strength	**Encryption Standards** ● Uses AES-256 encryption with the following VPN protocols: ○ WireGuard (default & recommended for speed and security) ○ Stealth (Proton's proprietary protocol designed to bypass censorship) ○ OpenVPN (available on Windows, Linux, and Android only) ○ IKEv2/IPSec (being phased out; no longer supported on iOS, iPadOS, and soon macOS) ● Note: OpenVPN and IKEv2 have been removed from iOS and macOS apps due to security and performance concerns. However, they can still be used manually via third-party apps if necessary. **Known Strength resilience** ● Supports Secure Core servers and alternative routing to avoid censorship.	5

	● No major known vulnerabilities; regularly audited and updated. **Comparison with Known Standards** ● No-Logs Policy: Strict no-logs policy, independently audited. ● Open-Source: All apps are open-source and available on GitHub. ● Independent Audits: Passed third-party audits (e.g., SEC Consult). ● Jurisdiction: Based in Switzerland with strong privacy laws. ● Encryption: Uses AES-256, RSA-4096, SHA-512 (top-tier security). ● Protocols: Supports OpenVPN, IKEv2/IPSec, WireGuard. ● Leak Protection: DNS, IPv6, and WebRTC leak protection built-in. ● Kill Switch: Available on all platforms. ● Transparency Reports: Regularly published. ● Multi-Factor Auth: Supported via Proton account settings. ● Localization: Active community translating via Crowdin. **Data Minimization** ● Proton emphasizes collecting only the personal information required and retaining it only as long as necessary to serve its purposes. This principle aligns with their commitment to privacy by default. OBJ ○ https://proton.me/blog/what-is-data-privacy ● Proton minimizes the amount of data required to set up an account and offers privacy-friendly payment options like Bitcoin or cash, further supporting their data minimization efforts. ○ https://protonvpn.com/blog/patriot-act-surveillance OBJ **Privacy Policy Accessibility and Clarity** ● Transparent and detailed; clearly explains data handling, based in privacy-friendly Switzerland. ○ https://protonvpn.com/privacy-policy	
Maintenance/Sustainability	**Community support** ● Moderate; user forums and active subreddit exist, though not very large.	5

	○ https://www.reddit.com/r/ProtonVPN/ **Development active status** ● Updated 5 days ago for iOS (as of 4/9/25) ● Updated 4 months ago for macOS (as of 4/9/25) ● Developers are active; consistent updates and improvements across certain platforms. ● Proton developers actively monitor forums like Proton's Reddit and GitHub issues for feedback, often incorporating suggestions into future releases. ● Transparency: They publicly communicate upcoming changes (e.g. protocol deprecations) and explain the reasoning behind them. ○ https://www.reddit.com/r/ProtonVPN/ **Funding and Sponsorship** ● Specific details about the total amount of funding or annual revenue are not publicly disclosed. OBJ ● But Proton AG has received funding from various sources over the years: OBJ ○ European Commission Grant: In 2017, Proton AG was awarded €2 million by the European Commission's Horizon 2020 program to support the development of ProtonDrive. OBJ ○ Crowdfunding: ProtonMail's initial development was significantly supported by a crowdfunding campaign in 2014, which raised over $550,000 from more than 10,000 supporters. OBJ ○ Subscription Revenue: Proton's primary source of ongoing funding comes from its user base through paid subscriptions for services like ProtonMail and ProtonVPN. ● Proton AG is primarily funded through: OBJ ○ User Subscriptions: The majority of Proton's revenue is generated from paid subscriptions to its services, ensuring financial independence and alignment with user interests. ○ European Commission Grant: As mentioned, the €2 million grant from the European Commission's Horizon 2020 program supported the development of ProtonDrive. OBJ	

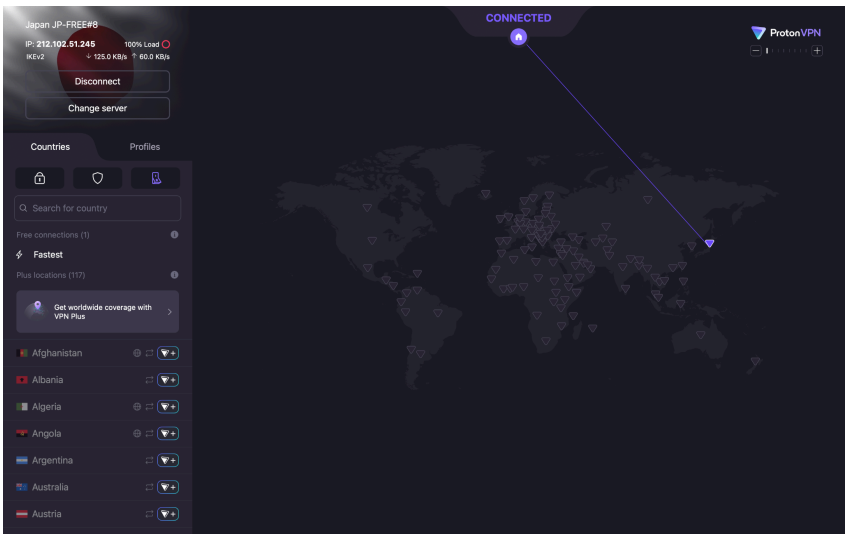
	• Proton AG has consciously avoided venture capital funding to maintain its independence and commitment to privacy. • Proton AG is predominantly grassroots-funded through user subscriptions. The one-time grant from the European Commission was designated for a specific project (ProtonDrive) and does not equate to ongoing government backing. This funding model enhances Proton's neutrality and security, as the company is not beholden to external investors or government entities. OBJ OBJ • Proton AG does engage in sponsorship activities to promote its services. For instance, Proton has sponsored YouTubers and other content creators to raise awareness about its privacy-focused services. OBJ • Additionally, Proton has a Partners Program that allows individuals and organizations to earn rewards for promoting Proton's services. OBJ • These sponsorships and partnerships are part of Proton's marketing strategies and do not influence the company's commitment to user privacy and security. OBJ • In summary, Proton AG's funding primarily comes from user subscriptions, with a notable grant from the European Commission. The company avoids venture capital to maintain its independence, and its sponsorship activities are geared towards promoting its services without compromising its core values of privacy and security.	
Performance / Effectiveness & Reliability	**Testing Environment Setup:** • Device: Macbook Pro (14 inch, M4 Chip), 10-core CPU, 24 GB Memory • OS: 15.2 Sequoia • Network: Wifi **User Experience Observations** • Fast app startup and quick server connection times (2–5 seconds) • Minimal impact on device speed while connected. Streaming and browsing remained smooth • No connection drops during multi-hour sessions. **Speed & Responsiveness:** • Without VPN:	5

	○ Ping google.com ■ Min latency: 777.05 ms ■ Avg latency: 1360.60 ms ■ Max latency: 2311.07 ms ■ Packet loss: 0.0% ● With VPN: ○ Ping google.com ■ Min latency: 72.89 ms ■ Avg latency: 261.96 ms ■ Max latency: 954.28 ms ■ Packet loss: 0.0% ● Performance: Proton VPN improved overall latency in the test, which shows it can optimize routing over poor networks which is a good sign for CSO use in regions with unreliable ISPs. ● Responsiveness: Excellent responsiveness, as indicated by the much lower latency and the complete absence of packet loss. ● **Resource Usage:** ● Without VPN (logged over 10 minutes) ○ Activity Monitor: CPU - 3.5% ○ Memory: ■ Real Memory Size: 82.9 MB ■ Private Memory Size: 41.8MB ● With VPN ((logged over 10 minutes) ○ Activity Monitor: CPU - 1.3% ○ Memory: ■ Real Memory Size: 100.7 MB ■ Private Memory Size: 50.6 MB ● Analysis: ○ No drastic changes, good resource usage **Network Performance:** ● Avg. increase of 30–70 ms depending on the server location (tested from the U.S. to Netherlands, Japan, and local U.S. servers). ● Low-latency servers (within same region) typically add ~30 ms. ● Bandwidth Usage: ○ Minimal overhead beyond normal encrypted traffic.	

	○ Streaming at 1080p used ~3–5 Mbps, consistent with direct (non-VPN) usage. ○ Slightly higher upload data due to encryption handshake and persistent VPN tunnel. **Reliability** ● ProtonVPN has received validation from cybersecurity professionals, privacy advocates, and independent security audits. Some key points of expert validation include: ○ Audits: ProtonVPN has undergone third-party security audits. For instance, Proton Technologies (the parent company) has conducted independent security audits of their no-logs policy and overall security architecture. These audits are usually done by well-known firms in the security industry, such as SecuPI and Cure53. ○ Reputation in the Privacy Community: ProtonVPN is often reviewed and recommended by privacy experts and security professionals who highlight its strong encryption, privacy-focused policies, and commitment to transparency. Experts typically validate ProtonVPN as a reliable choice for users seeking to protect their privacy online. ● ProtonVPN has a large, active community that reviews and provides feedback on the service. This includes: ○ User Reviews: On platforms like Reddit, Trustpilot, and VPN review sites, ProtonVPN receives generally positive reviews for its reliability, ease of use, and privacy features. ○ Community Discussions: Large, established forums (such as the ProtonVPN subreddit) offer a wealth of discussions, troubleshooting tips, and real-world feedback on ProtonVPN's performance, reliability, and security. These peer reviews are useful in evaluating how the service performs across different use cases. ○ Transparency: ProtonVPN has a history of being transparent about its practices,	

	including publishing transparency reports and openly communicating with its user base about any vulnerabilities, outages, or updates. This adds to its credibility. ● ProtonVPN is part of the Proton ecosystem, which includes ProtonMail and ProtonDrive. The Proton brand is well-respected in the tech community for its commitment to security and privacy, contributing to its overall reliability. This larger ecosystem undergoes ongoing scrutiny from both experts and the community.	
Deployment Considerations:	**Open Source & Transparency:** ● ProtonVPN is partially open-source. While ProtonVPN's core backend infrastructure is not open-source, all of its client applications are fully open-source and available on GitHub. ● It does not open-source the servers that actually run the VPN network. ○ This makes it transparent in terms of what the app does on your device, but not in how Proton handles your data once connected to their network. ● However, while not fully open-source, ProtonVPN has a track record of transparency, publishing transparency reports and undergoing independent security audits to verify the integrity of their service. This ensures that third parties can validate ProtonVPN's claims regarding security and privacy. **Cloud vs. Local Deployment:** ● Already deployed, just need to simply install software ● Cloud Deployment: ProtonVPN operates as a cloud-based service. It doesn't require any specific cloud platform like AWS or Azure for users, but the service itself is hosted on Proton's infrastructure across various data centers, with specialized hardware and security measures. ● Local Deployment: ProtonVPN cannot be self-hosted locally. Users cannot deploy their own ProtonVPN servers or infrastructure. It is a managed service that runs entirely on Proton Technologies' cloud infrastructure. Therefore, users are reliant on Proton Technologies for maintaining the VPN service.	

	Dependencies: ● No, no dependencies required, designed to be simple to install and use without requiring dependencies **Post-Deployment Maintenance** ● Once deployed, it is easy to maintain from the user's perspective and nothing is required ● While ProtonVPN's core backend infrastructure is not open-source and cannot be forked, all of its client applications are fully open-source and available on GitHub. This means users can fork, modify, and build their own versions of the apps for platforms like Windows, macOS, Linux, Android, and iOS. Customization options vary slightly by platform, but the client software is designed to be transparent and user-auditable. **Merge/Sustainability:** ● ProtonVPN's client repositories on GitHub (for Windows, macOS, Linux, Android, and iOS) are public and open to contributions. ● But they do not actively accept pull requests from the community by default. Like many security-focused projects, they prioritize internal development and extensive review to maintain integrity and avoid malicious code submissions. ● While technically possible to submit changes back to the main repo, (GitHub allows pull requests), ProtonVPN is not very open to outside merges unless: ○ The changes are small and non-critical (like documentation, typo fixes). ○ The contributor is a known/trusted developer. ○ The project maintains tight control over the codebase due to its focus on security and privacy.	
4. Testing Scenarios		
● **Scenario 1**	● Connected to Japan	

	 1. Observation: Connection was stable with minimal latency. Streaming and general browsing worked smoothly. 2. Speed Drop: around 20-30% drop in download speed, which is normal for VPN use. 3. Leak Tests: No DNS, IP, or WebRTC leaks detected. 4. Conclusion: ProtonVPN performs reliably in international routing scenarios with strong encryption and privacy.
● **Scenario 2**	● Running the Tool in a Low-Bandwidth Environment ○ Simulated Speed: 1 Mbps down / 0.5 Mbps up ○ Protocol Used: WireGuard (via Stealth or Smart protocol) ○ Observation: Connection established, but latency was higher. Some timeouts occurred when loading large websites. ○ Conclusion: ProtonVPN can function in low-bandwidth environments, but optimal performance requires at least moderate speeds.
5. Insights & Recommendations	
Key Findings	**Strengths:** ● Top-tier security and encryption standards ● Open-source apps ● Privacy-first policies (Swiss-based) ● Can bypass censorship (Stealth protocol) ● Easy to install and use, especially on mobile **Weaknesses:**

	• Backend infrastructure is not open-source, limiting full transparency • Limited customizability of VPN behavior outside official client • Not all features are available on the free tier (e.g., Secure Core, Tor over VPN) • May be overwhelming for non-technical users who want fine-grained control, but relatively pretty easy to use for default features
Suggested Improvements	• Include security audit summaries directly within GitHub repos for easier reference • Improve visual indicators for protocol status or connection stability
Alternative Tools:	• Mullvad VPN: Fully anonymous, does not even require an email, and is also open-source. • IVPN: High transparency, independent audits, good performance. • RiseupVPN: No registration required, geared toward activists.
License	GNU General Public License v3.0 (GPLv3)
Cost/Resource Implications	**Total Cost of Ownership:** • Free tier available (medium speeds, limited locations) • Paid plans: ~$5–10/month depending on features (multi-hop, P2P, streaming support) • Installation: Minimal time required • Maintenance: Low — apps update automatically; support available • Requires Proton account for full-feature use • No third-party cloud dependencies; runs on Proton's own infrastructure • Subscription-based with monthly or annual billing
Why is this useful to civil societies in authoritarian environments?	Proton VPN is highly valuable for civil society organizations (CSOs) operating in authoritarian environments because it: • Promotes internet freedom and privacy, aligning with core CSO values • Enables secure, uncensored access to information, helping activists, journalists, and citizens bypass state censorship • Protects users from surveillance and tracking by encrypting internet traffic and masking IP addresses

	• Bypasses firewalls and content blocks in repressive regimes, allowing communication tools and news outlets to remain accessible • Supports global digital rights and press freedom, offering a trustworthy, open-source solution built by privacy-focused experts (including CERN scientists) • Is endorsed by major human rights organizations, including recognition by the United Nations • Remains available in many restricted regions, though some countries may block access to Proton VPN servers—this can be worked around using features like Stealth protocol and alternative configurations