Synack

SECURE THE ELECTION OVERVIEW

WHY SECURE THE ELECTION

The right to a fair election has become a primary target of our adversaries. In the words of the Director of Department of Homeland Security's CISA, "We are doubling down on election security in advance of the 2020 election." The Secure the Election initiative is a bipartisan effort led by Synack, the leader in crowdsourced security testing, to bring together the best American security talent and tools to help our states build their attacker resistance. We believe that the best security comes from a united effort.

Together, we are offering states a pro bono crowdsourced security testing solution that augments security teams' efforts to find and fix security vulnerabilities in election systems before they can be exploited by the adversary. As part of this offer, Synack will also host a vulnerability disclosure program on behalf of the state. The majority of states have under 15 FTEs on their enterprise security teams, with <7% of states able to conduct third party penetration testing more than annually[1]. The crowdsourced security testing solution augments internal security teams with scale and provides on-demand testing and an assessment of security risk from an adversarial perspective.

WHAT WE TEST

Voter registration databases are a prime target for attackers. If exploited, an attacker could add, alter, or delete voter records, fundamentally affecting the outcome of the election. In 41 states, these systems are over ten years old, making them especially vulnerable to attack[2]. The National Association of Secretaries of State have flagged voter registration systems as a priority for upgrade[3].

This crowdsourced security testing solution looks for vulnerabilities in remotely-accessible voter registration databases and online voter registration websites from a hacker's perspective. We discover vulnerabilities left undetected by other solutions and help to remediate them before the election and before exploitation by the adversary. We look for:

- Which servers are connected to the internet?
- Does online voter registration connect to the voter registration database (VRDB)?
- Can admin access be gained? Can accounts be edited?
- Can VRDB be accessed through a 3rd party system (e.g., HHS, DMV)?

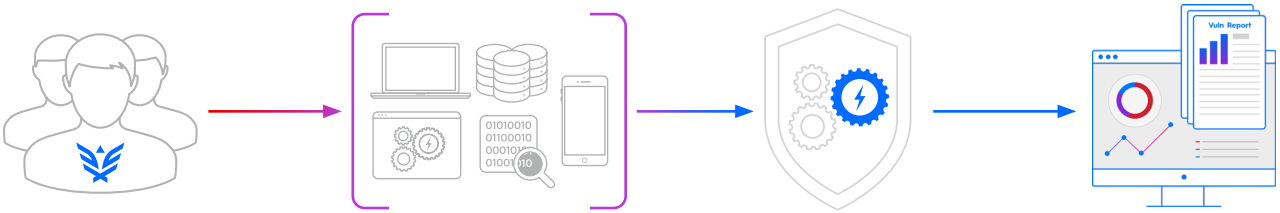
What you can expect from a Synack crowdsourced security test:

- **Trust:** Full control & visibility
- **Efficiency:** 24 hours to deploy, 24 hours to find severe vulnerabilities, 24 hours to triage
- **Quality:** >95% signal-to-noise ratio
- **Coverage:** >200 testing hours & 100s of security researchers in a 2-week test
- **Results:** Real-time analytics on results and asset hardness relative to peers
- **Partnership:** Force multiplier for your security teams

1 2016 Deloitte-NASCIO Cybersecurity Study.
2 Final Report, Congressional Task Force on Election Security, January 2018.
3 Final Report, Congressional Task Force on Election Security, January 2018

HOW CROWDSOURCED SECURITY TESTING WORKS

Synack, government's most trusted Crowdsourced Security Testing provider, uses a secure platform, vetted crowd of the top security researchers in the world and technical controls to provide the most effective and efficient testing solution with the least amount of risk. This approach was born out of our founders' offensive cyber experience at the NSA and has been engineered by top Silicon Valley talent.



Trusted Crowd of Security Researchers

5 step vetting process accepts only 10% of security researcher applicants:

1. Application Review
2. Behavioral Interview
3. Skill Assessment
4. Trust Assessment (Background & ID checks)
5. Continuous Monitoring

FVEY & SF-85P cleared researcher groups are available for government projects

Secure Platform

- Researchers must connect through Synack's secure gateway
- Synack tracks researcher activity & movement

Managed Testing

- Client scopes digital assets for testing and sets rules of engagement
- Synack's proprietary scanner conducts reconnaissance on the attack surface to increase the researcher efficiency 24/7 (365 days of the year.)
- Researchers test through the secure platform
- Researchers report vulnerabilities through the platform

Real-time Results

- Synack triages and prioritizes all vulnerabilities and shares findings in real time via the Client Portal
- Findings are shared with clients in real time via the Client Portal
- Synack researchers work with security teams to remediate rapidly

TRUSTED BY:

DoD & Civilian Agencies

F500 Banks & Credit Card Companies

Technology

Healthcare

eCommerce

> *"Synack's professionalism and our partnership during this program have provided immense value."*
>
> —SYNACK GOVERNMENT CUSTOMER

Terms & Conditions of the Secure the Election Pro Bono Offer:

This offer is limited to U.S. state governments. Each offeree will be eligible to receive one (1) free Synack Crowdsourced Vulnerability Discover test and one (1) free Synack Vulnerability Disclosure Program on an online voter registration, voting mobile application, or remotely-accessible database that is expected to be used in the upcoming 2020 Presidential election. Any website or database submitted for testing must be approved by Synack. Such approval may be withheld at Synack's sole discretion. Each test will be subject to Synack's standard terms and conditions. Synack reserves the right to cease or change this offer at any time.

Synack, Inc.

855.796.2251 | www.synack.com | info@synack.com

v2020.1—INT US