



LCSG

LITCHFIELD CYBER SECURITY GROUP

— DISCOVER. EXPLOIT. DEMONSTRATE. —

GOVERNMENT CYBER CAPABILITIES

DISCOVER. EXPLOIT. DEMONSTRATE.

Specialized offensive security and vulnerability research expertise for authorized U.S. Government cybersecurity and cyber operations requirements.

TECHNICAL DEPTH FOR COMPLEX MISSIONS.

LCSG brings hands-on offensive security, vulnerability research, adversary simulation and AI-accelerated analysis to mission-defined technical problems where conventional assessment approaches may not be sufficient.

Built Around the Objective

Government cyber requirements can differ significantly from commercial penetration testing. LCSG begins with the authorized mission objective, defines the technical problem precisely, and applies the offensive-security and research capabilities required to answer it.

OFFENSIVE SECURITY

Hands-on assessment and controlled exploitation of applications, APIs, infrastructure, cloud and identity environments.

VULNERABILITY RESEARCH

Deep investigation of complex technologies to identify previously unknown weaknesses, unconventional behaviors and exploitable attack paths.

ADVERSARY SIMULATION

Objective-driven operations that model realistic attacker progression across authorized systems and security boundaries.

BESPOKE TECHNICAL RESEARCH

Focused investigation designed around mission-specific technologies, protocols, environments and questions rather than a fixed service catalog.

**MISSION REQUIREMENTS DEFINE THE WORK.
TECHNICAL REALITY DEFINES THE APPROACH.**

Decades of Government Security Experience

LCSG's government capability is backed by founder Mark Litchfield's extensive historical experience conducting offensive security and vulnerability research for government and national-security organizations.

GCHQ SECURITY WORK

While co-founder of NGS Software, Mark performed security work for GCHQ. This historical work was conducted through NGS Software - not LCSG - and forms part of the experience behind LCSG's present-day government capability.

INVITE-ONLY U.S. GOVERNMENT SECURITY PROGRAMS

Mark has also participated in invite-only U.S. Government security initiatives, including Hack the Army, Hack the Marines and Hack the USAF.

SENSITIVE GOVERNMENT EXPERIENCE

His broader career includes sensitive security work supporting U.S. and U.K. intelligence and law-enforcement organizations. The specific organizations and nature of those engagements are intentionally not disclosed.

GOVERNMENT EXPERIENCE THAT PREDATES LCSG. TECHNICAL CAPABILITY THAT CONTINUES WITHIN IT.

Specialized Technical Support

LCSG can support authorized government requirements across multiple offensive-security disciplines. Specific scope, authorities and operational boundaries are established for each engagement.

APPLICATION & API SECURITY Advanced testing of web applications, APIs and service interfaces, including authentication, authorization, business logic and server-side attack paths.	EXTERNAL ATTACK SURFACE Technical discovery and assessment of internet-facing systems, services, cloud resources and other authorized externally reachable assets.
IDENTITY & ACCESS Assessment of authentication, tokens, federation, roles, privilege boundaries and identity-driven paths to sensitive systems.	CLOUD & INFRASTRUCTURE Testing of cloud services, exposed infrastructure, management surfaces, trust relationships and security boundaries.
NOVEL VULNERABILITY DISCOVERY Research intended to identify previously unknown or poorly understood security weaknesses in complex technology.	ATTACK-PATH DEVELOPMENT Controlled investigation of how individual weaknesses, identities and trust relationships can combine to achieve an authorized objective.

Disciplined Execution Within Defined Authority

Government cyber work requires clear authorization, operational discipline and evidence handling. LCSG structures engagements so that technical freedom exists within explicitly defined legal and operational boundaries.

01 AUTHORITY & OBJECTIVE

Confirm authorization, mission objective, target scope, permitted actions, prohibited actions and required outcomes.

02 TECHNICAL MODELING

Understand the target environment, technologies, attack surface, identities, trust relationships and relevant threat behaviors.

03 RESEARCH & DISCOVERY

Perform targeted technical research, reconnaissance and hypothesis-driven investigation within the authorized scope.

04 CONTROLLED EXPLOITATION

Validate significant weaknesses and attack paths only to the degree necessary to establish the required mission evidence.

05 IMPACT DEMONSTRATION

Document what access, control or security-boundary failure has been demonstrated without unnecessary operational impact.

06 TECHNICAL TRANSFER

Deliver findings, evidence, research artifacts and recommendations in the form required by the engagement.

Modern AI, Directed by Experienced Operators

LCSG embraces AI as a force multiplier for technical analysis and research. It can expand the volume of information examined and accelerate hypothesis generation, but mission decisions, exploit validation and operational judgement remain human-led.

AI CAN ACCELERATE

- Large-scale technical correlation
- Application, API and JavaScript analysis
- Protocol and data analysis
- Research hypothesis generation
- Attack-surface organization

EXPERIENCE DIRECTS

- Mission-focused prioritization
- Recognition of subtle security failures
- Selection of meaningful attack paths
- Controlled exploitation decisions
- Assessment of demonstrated impact

25+ YEARS OF OFFENSIVE SECURITY & VULNERABILITY RESEARCH EXPERIENCE

AI accelerates the work. Experience directs it - particularly when the requirement involves ambiguity, unconventional behavior or complex attack-path reasoning.

Authorization, Control and Discretion

LCSG's government capability is intended for explicitly authorized work. Engagement controls are adapted to the sensitivity of the mission and the environment.

EXPLICIT AUTHORIZATION Activities are conducted only under appropriate written authority and within agreed scope.	DEFINED BOUNDARIES Targets, permitted techniques, prohibited actions, safety constraints and stop conditions are established before execution.
NEED-TO-KNOW HANDLING Sensitive technical information and engagement artifacts are handled according to agreed access and retention requirements.	CONTROLLED VALIDATION Exploitation is limited to what is necessary to demonstrate the authorized objective or technical condition.
OPERATIONAL COMMUNICATION Clear points of contact, escalation paths and deconfliction procedures are established where required.	DISCREET EXECUTION Engagements can be structured to minimize unnecessary visibility or operational disturbance while preserving required evidence.

DELIVERABLES

Technical Evidence Built Around the Mission

Deliverables are tailored to the government customer and engagement objective rather than forced into a generic penetration-test template.

MISSION SUMMARY A concise explanation of the technical objective, scope, activity performed and outcome achieved.	TECHNICAL FINDINGS Detailed evidence of vulnerabilities, affected components, exploitation conditions and relevant security boundaries.
ATTACK-PATH ANALYSIS A reconstruction of how individual weaknesses and trust relationships combine to produce meaningful access or control.	RESEARCH ARTIFACTS Where applicable, technical notes, proof-of-concept material, indicators, test cases or other agreed research outputs.
IMPACT & LIMITATIONS Clear documentation of what was demonstrated, what was not attempted and the conditions required for exploitation.	REMEDIATION / MITIGATION Practical technical recommendations where defensive improvement is part of the mission requirement.

SPECIALIZED CAPABILITY. CLEAR AUTHORITY. MEASURABLE TECHNICAL OUTCOMES.



DISCOVER. EXPLOIT. DEMONSTRATE.

Specialized offensive security and vulnerability research capability for authorized U.S. Government cybersecurity and cyber operations requirements.

GOVERNMENT CYBER CAPABILITIES | RED TEAM OPERATIONS

PENETRATION TESTING | VULNERABILITY RESEARCH | M&A; CYBER DUE DILIGENCE

LCSG.US

LITCHFIELD CYBER SECURITY GROUP