Bantam Clean Power
A LODESTONE GROUP COMPANY

FLORIDA LOCAL GOVERNMENT | STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

Florida SLCGP
Compliance & Procurement Reference

Supporting documentation for Florida county, municipal, special-district, and law enforcement applicants funding Bantam Clean Power conditioning and Power Line Exfiltration (PLE) mitigation equipment under the federal State and Local Cybersecurity Grant Program (SLCGP).

Prepared for Florida local government technology leaders, including members of the Florida Local Government Information Systems Association (FLGISA).

Program	Federal State and Local Cybersecurity Grant Program (SLCGP)
Florida administrator	Florida Division of Emergency Management (FDEM), Grants Unit (State Administrative Agency)
Funding model	Pass-through sub-awards to local governments; applicants select their own budget items
Florida priorities	Critical Infrastructure (16 CISA sectors) and Law Enforcement; rural emphasis
Fundable capability	Every Bantam product conditions power and mitigates Power Line Exfiltration, closing NIST SP 800-53 PE-19 (Information Leakage)
This document is not	A grant application, an eligibility determination, or legal / compliance advice

Version 2.3 | June 2026 | Bantam Clean Power, a Lodestone Group company

READ FIRST

Important notice and how to use this document

Bantam Clean Power is an equipment manufacturer, not a grant administrator. This reference helps a Florida local government document, in its own application, the cybersecurity capability that Bantam equipment provides. Every Bantam product delivers a fundable capability; whether a specific purchase is approved is determined per application by the funding authorities, not by the vendor.

Allowability is determined by FDEM, CISA, and FEMA, per application
Equipment is an allowable SLCGP cost category when it addresses a cybersecurity risk or threat to information systems. The applicant states that connection in its justification, aligns it to Florida's approved Cybersecurity Plan, and the Florida Division of Emergency Management confirms the line item. There is no federal pre-qualified product list that approves a purchase in advance.
Program terms change each fiscal year, including cost-share percentage, priorities, and deadlines. Verify the current open cycle with FDEM before applying.

How to use this document in an application

- Attach it as vendor-supporting documentation behind the relevant budget line item.
- Use the framework mapping in Section 3 to draft your cybersecurity justification against the controls your agency is already required to meet.
- Use the cost-eligibility guidance in Section 5 to scope the purchase so it stays allowable equipment.
- Use the standards reference in Section 6 to document the specification you are buying.

THE PROGRAM

The SLCGP in Florida, in brief

The State and Local Cybersecurity Grant Program is a federal program created under the Infrastructure Investment and Jobs Act and administered jointly by two U.S. Department of Homeland Security components: the Cybersecurity and Infrastructure Security Agency (CISA), which provides cybersecurity subject-matter expertise, and the Federal Emergency Management Agency (FEMA), which provides grant administration. It is a four-year program funded across federal fiscal years 2022 through 2025, and its purpose is to help governments manage and reduce cybersecurity risks and threats to information systems they own or operate.

Only a state's designated State Administrative Agency may apply to FEMA. Local governments receive funding as pass-through sub-awards through the state; at least 80 percent of each state award passes through to local governments, and at least 25 percent reaches rural areas.

Florida administers the federal SLCGP through FDEM, not the Florida Digital Service
In Florida, the State Administrative Agency for the federal SLCGP is the Florida Division of Emergency Management (FDEM), Grants Unit, which publishes the application and submission guide. This is a separate program from the state-funded Local Government Cybersecurity Grant Program run by the Florida Digital Service (FL[DS]), under which capabilities are purchased centrally rather than distributed as cash. For the federal SLCGP described here, work with FDEM.

Florida priorities and eligibility

- **Critical Infrastructure (CI):** cyber hardening of systems such as SCADA, industrial control systems, operational technology, and associated IT infrastructure, across all sixteen CISA sectors.
- **Law Enforcement (LE):** cybersecurity risk mitigation for local law enforcement agencies that are not state agencies.
- **Rural emphasis:** a defined share of funding is directed to rural communities.

Eligible applicants are local governments: counties, municipalities, cities, towns and townships, local public authorities, school districts, special and intrastate districts, regional government entities, tribal governments, and rural or unincorporated communities. Nonprofits and private corporations are not eligible applicants. The grant is pass-through funding, and applicants describe their own budget, including intended purchases.

Program terms are set annually; confirm the current cycle with FDEM
SLCGP terms change each program year. The open funding cycle, application deadline, and local cost-share percentage have varied across years (recent local cost-share requirements have ranged from 20 to 40 percent), and applicants reapply for each year the program is offered. Before applying, confirm the current cycle, deadline, and cost-share figure with the Florida Division of Emergency Management, which publishes them on its SLCGP page.

THE JUSTIFICATION

Why every Bantam product is a fundable cybersecurity capability

Power Line Exfiltration (PLE) is the movement of data off a protected system over the building's power conductors. Because it travels the electrical path rather than the network, it bypasses firewalls and network monitoring and leaves no log entry. It is the physical-layer exposure that most agencies have left open.

Every Bantam product embodies the same patented architecture and therefore performs two functions at once: it conditions incoming power, and it suppresses signal transmission over the conductor, closing the PLE path at the outlet. This is an emanation-security control, which is exactly the kind of security protection the SLCGP is meant to fund.

One architecture, two functions, across the whole line
Bantam's active patents are embodied in every product: U.S. 8,223,468 ('Power Conditioning Circuit Utilizing High Oersted Rating Inductors') provides the conditioning function, and U.S. 11,775,645, 12,019,751, and 12,271,477 ('Suppression of Signal Transmission over a Conductor') provide the PLE mitigation function. Every Bantam unit is therefore both a power conditioner and a PLE mitigation solution; the cybersecurity case below applies to the entire catalog, not to a single model.

SLCGP objective alignment

SLCGP objective	How Bantam equipment supports it
Objective 3 (primary) Implement security protections commensurate with risk	PLE mitigation is a security protection against data exfiltration over the power path. It closes NIST SP 800-53 PE-19 (Information Leakage), a control most agencies have not otherwise addressed.
Objective 1 (supporting) Governance and continuity of operations	Where battery backup is included (Nexus family), the equipment also sustains the protective and monitoring systems that defend information systems through power disturbances and short outages.
Objective 2 (roadmap) Posture assessment and monitoring	Power-path anomaly detection is on the product roadmap and is the subject of a pending patent application. Treat it strictly as forward-looking; do not cite it as a present capability.

Framework mapping: controls your agency already has to meet

PLE mitigation supports controls and obligations that Florida agencies are already accountable to. Use the rows that apply to your agency to ground the justification in your existing compliance posture. Map each to your own specific obligations; the summaries below are a starting point.

Framework or obligation	What it calls for	How PLE mitigation supports it	FL priority
NIST SP 800-53 **PE-19** Information Leakage	Protect against information leakage from electromagnetic signal emanations.	Suppresses data-bearing emanations on the power conductor; directly addresses the control.	CI / LE
CJIS Security Policy	Protect Criminal Justice Information against unauthorized access and egress.	Closes a physical-layer egress path for systems handling CJI in law enforcement facilities.	LE
IRS Pub 1075	Safeguard Federal Tax Information against unauthorized disclosure.	Reduces an unmonitored disclosure path where FTI systems are processed (for example, tax and clerk offices).	CI
HIPAA Security Rule	Protect electronic protected health information with technical and physical safeguards.	Adds a physical-layer safeguard for ePHI systems in county health, EMS, and clinic settings.	CI
Florida **F.S. § 282.3185** Local Government Cybersecurity Act	Adopt cybersecurity standards consistent with the NIST framework and manage cyber risk.	Contributes a concrete control that strengthens the agency's documented risk posture.	CI / LE
AWIA (water systems)	Assess and address risk and resilience, including to control and electronic systems.	Hardens the power and signal path for SCADA and OT in community water systems.	CI

Be precise in the narrative: tie the purchase to the specific control and risk your agency carries, name the systems protected, and align it to your Cybersecurity Plan. The PLE / PE-19 framing is what ties the equipment to cybersecurity rather than to general electrical reliability.

THE EQUIPMENT

Bantam product line reference

The products below share the same conditioning and PLE-mitigation architecture and the same patent coverage; they differ in form factor, capacity, and whether battery backup is included. Request current datasheets and capacities for any model before quoting it in a budget.

Series	Models	Role / form	Listing
Tempest	SA3600	Conditioning and PLE-mitigation building block	UL 62368-1 (component)
Citadel	RM1440A, RM2880A	Rack-mount conditioning and PLE-mitigation units	UL 62368-1 listed
Vanguard	PP3002B, PP3004A, PP18004A	Point-of-use conditioning and PLE-mitigation units	UL 1449 listed (MET Labs)
Nexus UPS	360, 800, 1200, 1500	Clean-power UPS; adds battery backup continuity	UL 1778 evaluation in progress

Preliminary electrical ratings
Exact electrical ratings, including capacity, runtime, and transfer time for the Nexus units, are being finalized and are preliminary. Request the current datasheet for any model before quoting it.

ALLOWABLE COSTS

Scoping the purchase so it stays an allowable cost

Equipment is allowable when it addresses a cybersecurity risk or threat to information systems. How the equipment is deployed matters as much as what it is.

Keep it personal property: do not hard-wire it into the building
FEMA generally treats work that modernizes a building's electrical infrastructure (replacing panels, upgrading wiring, replacing breakers) as an unallowable building alteration, and affixing equipment so it becomes a permanent part of the building can also remove its personal-property status.
Deploy Bantam units as cord-connected, rack-mounted or free-standing equipment that plugs into existing receptacles. Avoid permanent electrical installation, and do not bundle building electrical upgrades into the grant line item.

Other cost rules to plan around

- **Cost share.** A local match is required; confirm the current percentage with FDEM and budget the non-federal share. Grant funds cannot cover your own cost-share contribution.
- **No supplanting.** Funds must add to, not replace, money you would otherwise spend.
- **Period of performance.** Costs must be incurred, and equipment received and put to use, within the grant's period of performance; plan procurement and delivery timelines accordingly.
- **Direct cybersecurity nexus.** Any item that does not address a cybersecurity risk or threat to information systems is unallowable. Lead with the PLE / PE-19 nexus, not reliability alone.

STANDARDS & CERTIFICATION

Standards and certification reference

The statements below are conservative and current as of the version date. Do not represent any in-progress evaluation as a completed listing.

Item	Status	Notes
Tempest SA3600 conditioning component	**UL 62368-1 listed** (component level)	UL 62368-1 is the safety standard for information and communication technology equipment. This is the conditioning and PLE-mitigation building block carried across the line.
Citadel series (RM1440A, RM2880A)	**UL 62368-1 listed**	The rack-mount conditioning and PLE-mitigation units carry the same product-safety listing.
Vanguard series (PP3002B, PP3004A, PP18004A)	**UL 1449 listed** by MET Labs	UL 1449 is the standard for Surge Protective Devices. MET Laboratories is an OSHA-recognized Nationally Recognized Testing Laboratory (NRTL).
Nexus UPS systems (360, 800, 1200, 1500)	**UL 1778 evaluation in progress** (not yet listed)	UL 1778 is the standard for Uninterruptible Power Systems. A component listing does not by itself certify a finished UPS; do not claim a finished-system UL listing until it is issued.

Item	Status	Notes
Battery subsystem (Nexus)	Listing path under evaluation	The applicable listing approach (cell-level versus system-level) is being determined.
Electromagnetic / PLE performance	Documented on request	Request current test documentation for any emissions or PLE-attenuation figures used in an application.

For certification evidence in an application or procurement file, request a current, dated certification letter from Bantam Clean Power rather than relying on this summary.

BEFORE YOU APPLY

Applicant readiness checklist

- ☐ Confirm your entity is an eligible Florida local government applicant.
- ☐ Confirm the current FDEM application cycle, deadline, and cost-share percentage.
- ☐ Identify whether your project fits Critical Infrastructure or Law Enforcement, plus rural emphasis.
- ☐ Select the framework rows in Section 3 that match your agency's obligations (PE-19, CJIS, IRS 1075, HIPAA, F.S. 282.3185, AWIA).
- ☐ Draft a justification tying PLE mitigation to a specific control, risk, and SLCGP objective.
- ☐ Confirm alignment with Florida's approved Cybersecurity Plan through the required process.
- ☐ Scope the equipment as cord-connected personal property; exclude any building electrical alteration.
- ☐ Budget the non-federal cost-share match; do not fund the match with grant dollars.
- ☐ Request current datasheets and a dated certification letter from Bantam Clean Power.
- ☐ Attach this reference and the vendor quote as supporting documentation, and confirm each line item with FDEM.

REFERENCE

Intellectual property and contacts

Patent reference

Every Bantam product is covered by the company's active patent portfolio: U.S. 8,223,468 (power conditioning circuit) and U.S. 11,775,645, 12,019,751, and 12,271,477 (suppression of signal transmission over a conductor). Additional applications are pending. Patent coverage is provided for procurement records; it is not a representation about grant allowability.

Where to apply and verify program terms

Resource	Use it for
Florida Division of Emergency Management, Grants Unit floridadisaster.org (SLCGP page) · 2489 Shumard Oak Blvd, Tallahassee, FL 32311 · 850-815-4000	The authoritative Florida application, submission guide, current cycle, deadline, cost share, and allowability questions.
CISA, State and Local Cybersecurity Grant Program cisa.gov/cybergrants/slcgp	Federal program objectives, best practices, and the current Notice of Funding Opportunity.
Florida Digital Service, Local Government Cybersecurity Grant Program cybersecuritygrants@digital.fl.gov	Awareness only: the separate, state-funded capabilities program, distinct from the federal SLCGP.
Bantam Clean Power Mike Januszewski · michaelj@bantamcleanpower.com · (630) 929-3050	Current datasheets, dated certification letters, configuration guidance, and quotes.

Document control

Version 2.3 | June 2026. Prepared by Bantam Clean Power, a Lodestone Group company. Provided for informational purposes to support a local government's own SLCGP application. It is not a grant application, an eligibility or allowability determination, or legal, financial, or grant-compliance advice. Program terms, cost-share percentages, deadlines, priorities, and product certifications change over time; confirm current details with the Florida Division of Emergency Management and request current product documentation from Bantam Clean Power before relying on anything herein.