RESPONSE TO NON-FINAL OFFICE ACTION Application No.: 17/741194 Filing Date: 05/19/2022 Art Unit: 2645 Examiner: OBAYANJU, OMONIYI Title: SELF-CONTAINED DISASTER CONDITION MONITORING SYSTEM Applicant: Daniel Kenney (Pro Se) Date of Response: [Insert date of filing]

PRELIMINARY REMARKS Applicant respectfully submits this response to the Non-Final Office Action dated March 12, 2025. This submission includes a complete replacement of the claims to reflect a focused reevaluation of the actual inventive contribution disclosed in the specification.

After assuming personal responsibility for prosecution, Applicant reviewed the claims with a more critical eye and recognized that the earlier claim set consisted primarily of claims from the original application. This CIP was always intended to focus on the new innovation—namely, a secure, app-free SMS-based control model—and the revised specification reflected that. Unfortunately, the claim set drafted by prior counsel did not incorporate the substance of this new material. Applicant regrets the resulting inefficiencies and appreciates the Examiner's patience and effort in working through the previous record.

As a pro se applicant, Applicant respectfully requests the consideration outlined in MPEP § 707.07(j) regarding support and clarification for pro se inventors. in navigating the earlier stages of this application and hopes this submission marks a more productive and focused phase of examination. As a pro se applicant, Applicant respectfully requests the consideration outlined in MPEP § 707.07(j) regarding support and clarification for pro se inventors.

AMENDMENTS TO THE CLAIMS Please cancel all previously pending claims and replace them with the following new claims 1–10. The revised claims are directed solely to the core innovative contribution: a system that binds an authorized user via SMS and receives configuration and command instructions through direct SMS communication alone, without requiring app-based interfaces, internet connectivity, or physical proximity.

1. A communication-enabled electronic device comprising:
- a processor;
- a GSM modem coupled to a SIM card with an active telephone number;
- a non-volatile memory;

wherein the processor is configured to:

- receive an SMS message comprising a device-specific authorization code;
- authenticate the authorization code;
- upon successful authentication, store the originating telephone number as an authorized user;
- accept subsequent SMS messages from authorized users comprising configuration parameters or operational commands;
- execute received commands or apply configuration parameters to modify the behavior of the device;
- and reject or delay further authorization attempts after a defined number of failures.

2. The device of claim 1, wherein the processor maintains a configurable list of authorized users, each with individual permissions.
3. The device of claim 1, wherein the processor responds to SMS commands to query configuration status, update configuration values, request sensor readings, or initiate system reset.
4. The device of claim 1, further comprising one or more sensors, and wherein the processor is further configured to:
- poll the sensors;

- compare readings to stored thresholds;
- and transmit alert SMS messages to authorized users upon threshold exceedance.

5. The device of claim 4, wherein the sensors detect disaster-related conditions including water, temperature, smoke, or gas.
6. The device of claim 1, wherein the processor issues periodic status reports via SMS to authorized users.
7. The device of claim 1, wherein the device operates independently of any user-facing application or internet connection.
8. The device of claim 1, wherein the device is deployable without physical interaction beyond initial power-up, and is fully operational once the authorization SMS is received.
9. The device of claim 1, wherein the processor is further configured to:

- filter rapid or repeated SMS submissions to reduce the risk of brute-force attacks; and
- evaluate sender identity using heuristics beyond caller ID to mitigate spoofing risk.

10. The device of claim 9, wherein the processor uses timing-based or behavioral analysis to determine legitimacy of incoming SMS messages.

REMARKS The revised claim set is rooted in the actual inventive contribution disclosed in the specification: a lightweight, UI-free method for remote user authorization and control of an electronic system via direct SMS. This model enables secure, rapid deployment in disaster scenarios or infrastructure-limited contexts, without apps, internet, or pre-paired interfaces.

The invention is not the GSM modem or the SIM card themselves. Rather, it is the *method by which control is established and exercised* using only SMS—a model that allows any user to activate and configure the system securely with a single message, regardless of location.

The cited references fail to disclose or suggest this user pairing model:

- Balaji et al. do not teach configuration via SMS.
- McCrosky involves GSM telemetry, but lacks dynamic user authorization or command logic via SMS.
- Dizengof describes carrier selection, not control flow.
- Ward and Catlin are concerned with sensing and detection, not communications architecture.

Applicant respectfully traverses the 35 U.S.C. § 103 rejections. While this system does not claim cryptographic security methods, it does specify a first layer of SMS-based access control, which skilled practitioners may supplement with standard protections as needed. These enhancements are implementation details—not part of the core inventive structure.

If the Examiner believes that any subject matter is allowable in dependent form, Applicant is open to interview or amendment to expedite prosecution.

Respectfully submitted,

Daniel Kenney (Pro Se) dankenney524@gmail.com 321-298-8999 [Insert Date]