THE NEW ESTATE STANDARD INSTITUTE

Luxury Homes in the Era of AI

A Technical White Paper on Privacy, Security, Cyber Resilience, Clean Air, Protected Infrastructure, and Continuity for High-Value Residences

NES Certified™

AI-Era Residential Resilience Certification

Published by The New Estate Standard Institute LLC
Technical White Paper · Version 1.0 · 2026
An educational & informational research publication

ABOUT THIS PAPER

This is the full technical white paper behind The New Estate Standard Institute's public education materials, buyer guides, and NES Certified™ evaluation framework. It is written for the people who want the evidence base behind the framework: builders, luxury real-estate agents, family offices, private-wealth advisors, security consultants, architects, and serious buyers of high-value residences.

Its argument is narrow and evidence-led. The risk environment around high-value homes is changing, the AI era is a meaningful part of why, and a recognizable design response is emerging. The paper is not a sales document, does not promote any specific property, and reaches no conclusion that a home can be made safe.

PUBLISHER NOTE

The New Estate Standard Institute LLC publishes research and frameworks related to AI-era residential resilience. This white paper is educational and informational. It does not provide legal, security, cybersecurity, engineering, insurance, HVAC, fire, medical, or other professional advice. No home can be guaranteed safe, secure, immune from attack, or protected against all risks. NES Certified™ evaluates alignment with a residential resilience framework; it does not guarantee safety, security, code compliance, insurance acceptance, or threat prevention.

A NOTE ON EVIDENCE STANDARDS

This paper deliberately separates five kinds of statements and signals which is which throughout:

- **Documented fact** - events and figures reported by primary sources, government agencies, or court records.
- **Reported allegation** - claims that are the subject of investigation or prosecution and have not been adjudicated; described here as alleged, suspected, or charged.
- **Expert warning** - concerns stated publicly by the institutions closest to a given technology.
- **Forward-looking inference** - reasoned extrapolation from documented trends, framed as inference rather than prediction.
- **Design recommendation** - architectural and engineering responses that follow from the evidence.

Where a claim is contested, this paper attributes it and prefers to under-claim. No statement here should be read as a guarantee of any outcome. A full disclaimer appears at the end of this document.

Contents

BRIEFING

Executive Summary

A The standard is changing

High-value residential real estate is entering a standards shift. For much of the last century, luxury homes were judged primarily by what could be seen: location, views, scale, glass, finishes, amenities, and photography. Those attributes still matter. But the AI era is changing what a serious private residence must protect.

Safety standards have always moved when the environment moved. Seat belts, residential fire systems, alarm systems, doorbell cameras, smart locks, hurricane glazing, seismic design, and protected rooms each became more normal as the world around the home changed. The conditions around high-value residences are changing again, and the design response is becoming a standard of its own.

B Why AI matters

Artificial intelligence does not create most of these risks; it changes their economics. Reconnaissance, social engineering, pattern-of-life analysis, network probing, impersonation, and data aggregation each used to require time, skill, and people. AI lowers the cost and the expertise required for all of them.

The relevant pattern is not a single new weapon. It is a broad reduction in the effort needed to study a household, defeat a countermeasure, or run an attack at scale - which moves capabilities that once belonged to organized or state-level actors within reach of ordinary bad actors.

C Why high-value residences are differently exposed

At the $5M, $10M, $20M, and $30M level, a residence is not merely a lifestyle asset. It functions as a private operating environment for a high-value household: family routines, valuables and vehicles, staff and vendor access, confidential documents, networked infrastructure, business exposure, and reputational risk concentrate under one roof. At a certain level, the home itself becomes a signal.

This does not imply that every wealthy household is targeted. It does imply that the risk profile is materially different from that of an ordinary residence - and that the difference is now legible to automated tools.

D What the evidence shows

The evidence is already in public reporting and government records. Federal law enforcement has described organized crews that study a family in advance - mining public records and social media to build a "pattern of life" - before defeating alarms and cameras with off-the-shelf Wi-Fi jammers.[1, 2, 3]Americans reported $16.6 billion in internet-crime losses in 2024, up a third in a year.[16, 17]In November 2025, a documented campaign used a frontier AI tool to conduct cyber-espionage that targeted roughly thirty organizations, with the model performing an estimated 80-90% of the work.[18, 19]Aerial privacy is constrained by airspace law a private owner cannot override.[12, 13]Unlicensed laboratories have been discovered operating from American residences.[31, 45, 46]And in January 2025, wildfire destroyed a large share of some of the most expensive housing in the country, where engineering - not finish quality - separated the homes that survived from those that did not.[34, 35]

E What the new standard should include

The response is not a bunker. It is the next standard of luxury: privacy by architecture, layered physical security, cyber-resilient smart-home design, a protected core, clean-air capability, backup power, independent communications, environmental resilience, and disciplined vendor and staff access governance.

F Why design timing matters

Most of these capabilities are inexpensive as lines on a drawing and expensive - or impossible - as retrofits. Structure, network backbone, sightlines, and a protected core are design decisions, not accessories. The practical question is therefore not only what to build, but when the decision is made: before the slab is poured, or after.

G How the 52-question framework responds

To make the standard testable rather than rhetorical, this paper closes with 52 questions across six categories - the 52-Point AI-Era Residential Resilience Framework. Those questions form the public basis of NES Certified™, the Institute's AI-Era Residential Resilience Certification: a structured, documentation-supported evaluation of how well a residence aligns with the practices described here. The framework measures alignment with a standard; it does not, and cannot, guarantee an outcome.

H Call to action

Buyers, builders, advisors, and agents are encouraged to evaluate high-value homes under an AI-era residential resilience framework - to ask the 52 questions early, while they can still be answered with a pencil, and to treat privacy, security, cyber resilience, clean air, and continuity as part of what the word luxury now means.

SECTION 01

Why High-Value Residences Are Differently Exposed

A high-value residence differs from an ordinary home not only in price, but in what it concentrates and what it signals. The design question that follows is not whether a household is wealthy, but what its home implies to an observer who is increasingly a machine.

At a certain level, the home itself becomes a signal. Scale, location, and visibility communicate that a household is likely to hold concentrated assets and valuable contents, to travel, to employ staff and engage many vendors, to own or run a business, to keep confidential documents, and to carry reputational and family exposure. Each of these is, in security terms, an attack surface.

The relevant factors are straightforward to enumerate:

- **Asset and contents concentration** - art, jewelry, vehicles, watches, and cash equivalents gathered in one location.
- **Travel and absence patterns** - predictable periods when a residence is empty, increasingly inferable from public information.
- **Staff and vendor complexity** - a larger population of people and companies with physical or network access than an ordinary home has.
- **Public visibility** - named ownership, published architecture, prior real-estate listings, and media presence.
- **Business and financial exposure** - a household that transacts and delegates at scale presents more opportunities for impersonation and fraud.
- **Confidential documents and family leverage** - records whose exposure carries legal, financial, or personal consequences beyond their replacement cost.

> *The point is not that wealth invites attack. It is that wealth changes the risk profile - and that AI makes that profile easier to read from the outside.*

This does not mean every high-value household is targeted, and the paper makes no such claim. It means the practical question for a high-value residence is different from the one an ordinary home faces. The remainder of this paper sets out the evidence, category by category, and the design response each category implies.

SECTION 02

The Evidence, Category by Category

Each category below pairs documented evidence with the design implication that follows from it. The evidence is drawn from government, primary, academic, and reported sources; the design recommendations are the engineering and architectural responses those facts suggest.

CATEGORY 01

Physical Security

The clearest official description of how high-value homes are currently targeted comes from federal law enforcement, and it describes intelligence work rather than opportunistic burglary. In December 2024, the FBI formally warned major professional sports leagues after organized crews burglarized the homes of at least nine professional athletes over roughly three months, among them Patrick Mahomes, Travis Kelce, Joe Burrow, and Luka Dončić.[1, 3]

According to the bureau, the crews - which federal and local investigators have linked to South American Theft Groups (SATGs) - conduct surveillance in advance, mine public records and social media to build a "pattern of life," and frequently establish where valuables are kept before entering. They then defeat alarms and cameras using off-the-shelf Wi-Fi jammers and signal blockers, and leave within minutes.[1, 2, 3]The bureau also noted that some of these burglaries occur while residents are home, and advised avoiding confrontation because crews may be armed.[2]

130+

ARIZONA "DINNERTIME" BURGLARIES TIED TO ONE PATTERN SINCE LATE 2023

Scottsdale, Paradise Valley, Phoenix, Gilbert, and Chandler were all affected; many victims had alarms and cameras and had simply left for the evening.[7, 8, 9]

The pattern is documented well beyond celebrity victims. In Los Angeles, the police department recorded more than 900 residential burglaries in a single year and established a dedicated task force; investigators attributed roughly a hundred break-ins in one period to these groups.[5]Ventura County attributed 175 residential burglaries to transnational theft groups between 2019 and mid-2023.[5]In federal court, prosecutors described a Southern California ring that flew in "crime tourists" on visa-waiver entries and directed them where to strike, with one operator accused of moving more than $5 million in stolen goods.[6]

Arizona sits squarely within this pattern. Crews described in local reporting as "Dinnertime Burglars" were tied to more than 130 incidents in and around Scottsdale beginning in late 2023, with Paradise

Valley, Phoenix, Gilbert, and Chandler also affected.[7, 8]The geography of entry is itself a design lesson: crews used golf-course frontage and desert washes to reach the rear of properties, because a gate controls the entrance and does little for the back of a lot.[7]In related Southern California cases, residents discovered surveillance cameras concealed in landscaping, and suspects were reported wearing camouflage while waiting in vegetation.[10, 11]Scottsdale police characterized the operators as professionals and emphasized that many victims had alarms and cameras and had simply left the house for an hour or two.[8, 9]

> *The relevant question is not whether a property has cameras and alarms, but whether those systems still function when their connection to the outside world is cut from the street.*

Why AI sharpens this

Two mechanisms make this category more acute, and both are documented. First, reconnaissance - historically the expensive, time-consuming part of a sophisticated burglary - is increasingly automated. A household's own published information (location-tagged posts, travel updates, cached real-estate listings with full interior walkthroughs, permit records, flight-tracking data on private tail numbers) can be aggregated, summarized, and put on a timeline by automated tools far faster than by a person. The FBI explicitly identified publicly available information and social media as the crews' targeting inputs.[1]Second, the tools used to defeat countermeasures are now commodity hardware; the bureau named Wi-Fi jammers, signal blockers, and camera-defeating devices as standard SATG equipment, and AI assistance lowers the skill required to identify and exploit a specific installation.[2]

DESIGN IMPLICATIONS

The design response treats the lot, the network connection, and the information footprint as one perimeter.

- Treat the true lot perimeter - washes, golf frontage, service alleys, adjacent construction - as the security boundary, not the gate.
- Specify cameras and alarm components that store and verify locally and fail to a safe state when connectivity is jammed, rather than systems that go blind when Wi-Fi drops.
- Use wired cameras on a wired network for the security layer; reserve wireless for convenience.
- Provide a true safe room engineered to recognized standards (see Category 04), not a reinforced closet.
- Manage the household's information footprint with the same rigor as its physical perimeter: remove interior listing photography after a sale, limit real-time location disclosure, and assume published details are read by automated systems.

CATEGORY 02

Privacy

A perimeter wall addresses a person standing on the ground. It does not address a small consumer drone - often costing little more than $1,500 - hovering at altitude with a stabilized zoom camera, and current law largely favors the operator.

The legal framework is less protective than many owners assume. In United States v. Causby (1946), the Supreme Court held that navigable airspace is a public highway and that a landowner controls only the "immediate reaches" of the airspace they can actually use; the Court declined to set a precise boundary, but the case concerned flights as low as 83 feet.[12]Modern drone regulation inherits this directly: the FAA controls navigable airspace, and recreational and commercial operators may generally overfly private property when following applicable rules.[13]

The interdiction options available to a private owner are constrained by federal law. Disabling a drone by force is generally prosecutable: drones are classified as aircraft, and damaging an aircraft is an offense under 18 U.S.C. § 32.[14]Jamming a drone's signal is also prohibited; the FCC bars signal jammers, with substantial penalties, and only specified federal agencies are authorized to employ counter-drone measures.[15]The privacy protections that might otherwise apply are a patchwork of state and local rules that are difficult to enforce and generally require first identifying the operator and what was captured.[13]

> **83 ft**
>
> **LOWER BOUND OF PROTECTED AIRSPACE AT ISSUE IN CAUSBY (1946)**
>
> Above the immediate reaches of the land, airspace is treated as a public highway; a private owner generally cannot lawfully intercept an overflying drone.[12, 14, 15]

This is not speculative concern. Federal agencies have flagged certain foreign-manufactured drones as a national-security risk to critical infrastructure specifically because of what they can observe and where the resulting data may be transmitted.[43]If the government treats a commodity drone's observation and transmission as a risk to infrastructure, the implication for a private estate follows directly.

Why AI sharpens this

Aerial imagery becomes a security concern at the point it is converted into an actionable plan, and that conversion is exactly what machine vision now automates. Footage that was once merely scenic can be processed into a labeled site survey: entry points, camera placements and blind spots, skylights, mechanical equipment, and the timing of lights and vehicle movement. The analytical step that previously required a human is increasingly performed automatically.

> *Privacy at this level is an architectural property, not a fence property. The airspace cannot be controlled; only the building can.*

DESIGN IMPLICATIONS

Because the airspace cannot be controlled, privacy has to be designed into the building.

- Design sightlines so that the most-used private spaces (primary suite, pool, glass-walled rooms) are not observable from the airspace a drone may lawfully occupy - using roof overhangs, louvered screens, courtyard orientation, mature canopy, and pergola structures as visual baffles.
- Where the program allows, an interior-courtyard scheme provides open-air living that is private from both street and sky.
- Specify glazing and window treatments on the assumption that any window facing open sky also faces a camera.
- Where appropriate to the property, consider lawful drone-detection - not interdiction - so that overflights are at least known.

CATEGORY 03

Cybersecurity

The anchoring figure is $16.6 billion: the amount Americans reported losing to internet crime in 2024, a 33% year-over-year increase across nearly 860,000 complaints, with phishing and spoofing the most common methods and people over 60 - a demographic that disproportionately owns high-value homes - reporting the heaviest losses.[16, 17]Business email compromise, in which an attacker impersonates a trusted party to redirect a payment, accounted for $2.77 billion on its own.[16]Wealth concentrates this exposure: the more a household transacts, delegates, and grants account access to staff and vendors, the larger its attack surface.

A modern luxury residence is, in practice, a networked environment with a large device population: lighting, climate, shades, locks, cameras, audio, irrigation, gates, pool, wine storage, and art sensors - many of them cloud-dependent and shipped with weak default security. Each connected device is a potential entry point, and these devices are being compromised at scale.

The relevant incidents are well documented. In 2024, the FBI, NSA, and CISA disclosed a botnet operated by a China-based company that had compromised hundreds of thousands of consumer devices - home and small-office routers, IP cameras, DVRs, and network-attached storage - with one snapshot exceeding 260,000 devices and more than 385,000 U.S. devices over its lifetime.[20, 22]The Volt Typhoon campaign, attributed to a PRC actor, has pre-positioned inside critical infrastructure by exploiting the same classes of home and small-office routers found in millions of residences.[43]The earlier Mirai botnet spread simply by trying default usernames and passwords on internet-connected cameras and routers, enslaving hundreds of thousands of devices.[21]And in June 2025 the FBI warned that some consumer devices - streaming boxes, projectors, and digital picture frames - were arriving already infected and conscripted into criminal networks on first use.[23]Compromise did not require carelessness; it required only purchasing the device and connecting it.

$16.6B

U.S. INTERNET-CRIME LOSSES REPORTED IN 2024 (UP 33% YEAR OVER YEAR)

Across nearly 860,000 complaints; business email compromise alone accounted for $2.77 billion.[16, 17]

AI changes the economics of this category in a documented way. In November 2025, Anthropic reported that a Chinese state-sponsored group had manipulated its Claude Code tool into conducting a cyber-espionage campaign that targeted roughly thirty organizations worldwide - technology companies, financial institutions, chemical manufacturers, and government agencies - with the AI performing an estimated 80-90% of the work, including network mapping, exploit development, credential harvesting, and data exfiltration, at request rates no human team could match.[18, 19]The method for bypassing the model's safeguards was notably simple: the operators told it that it was an employee of a legitimate security firm running defensive tests, and broke the malicious work into small, innocuous-looking tasks.[18]Anthropic characterized this as an escalation from earlier cases in mid-2025 in which humans still directed most of the work; the same firm had previously identified North Korean operatives using its model to obtain remote employment at U.S. companies under false identities.[19, 44]The significant point is not that one provider had an incident, but that the capability now exists in the wild - and capability proliferates.

> *Cybersecurity at this level is residential security. A networked home with default passwords, a flat network, and several vendors holding standing access is the digital equivalent of issuing keys to strangers.*

DESIGN IMPLICATIONS

The design response treats the home network as critical infrastructure, segmented and governed rather than flat and open.

- **Network segmentation.** Family devices, the security system, and smart-home devices should occupy separate, isolated network segments (VLANs), so that a compromised device cannot reach cameras, locks, or the systems used for email and finance. CISA's guidance is, in effect, to treat IoT devices as untrusted.[23]
- **A business-grade hardware firewall** - not the internet provider's default router - to inspect traffic and enforce rules between segments.
- **A hardwired backbone.** Structured cabling cannot be jammed from the street, is harder to intercept, and does not broadcast the network's presence. Wi-Fi is reserved for convenience, never the security layer.
- **VPN architecture for remote access,** so that owner, staff, and vendor access runs through an encrypted tunnel into a controlled entry point rather than many separate cloud apps.

- **Encrypted, air-gapped storage** for irreplaceable records, with the most sensitive copy physically disconnected from any network.
- **Vendor access governance.** Every integrator and platform with access should hold unique, revocable, least-privilege credentials with multi-factor authentication and a logged trail; no installer should retain a permanent master key.
- **Changed defaults and a living device inventory,** maintained - ideally under contract - across firmware and credentials over time.

CATEGORY 04

The Protected Core

A useful precedent for this section already exists, built by the U.S. government. The Greenbrier facility - a continuity-of-government bunker constructed beneath a West Virginia resort between 1958 and 1962 and kept secret until 1992 - combined, behind blast doors, decontamination chambers, dormitories, an independent power plant, large stored water and fuel reserves (three 25,000-gallon water tanks and three 14,000-gallon fuel tanks), a communications center, a clinic, and a rotating food supply.[37, 38, 39] The lesson is not that a residence needs a Cold War bunker; it is that when a highly security-conscious organization was asked to design a space to survive almost anything, it produced a single hardened room that integrated protection, power, water, communications, medicine, and data.

A modern luxury home can apply the same principle in residential form: one hardened core engineered to serve simultaneously as a safe room during an intrusion; a server and communications room that keeps the network and connectivity alive when the rest of the house is compromised or without power; a data and document vault holding the encrypted, air-gapped copy of what is irreplaceable; a redundant control center for the home's systems; and a shelter with independent, filtered air and independent power.

This is an engineering proposition, not a survivalist one. The relevant standards already exist and are mainstream: FEMA's safe-room guidance (P-361 and P-320) and the ICC 500 standard define what a protected space must do to provide what FEMA terms "near-absolute protection," including resisting design wind speeds up to 250 mph and the impact of a 15-pound 2×4 traveling at 100 mph.[40, 41] Builders already construct rooms to this standard, and appraisers and insurers already recognize them.[41] What is new is the argument for consolidating the security, data, and resilience functions into one shell rather than scattering them across a network closet, a wall safe, and a nominal panic room.

250 mph

DESIGN WIND SPEED FOR FEMA / ICC 500 "NEAR-ABSOLUTE PROTECTION"

The same standards require withstanding a 15-lb 2×4 impact at 100 mph; rooms built to them are already recognized by appraisers and insurers.[40, 41]

IMPLEMENTATION, IN SEQUENCE

Because the shell is structural, the sequence in which these decisions are made determines their cost.

- **Design it in during architecture.** A protected core is a structural decision - a reinforced concrete or CMU shell, a vault-rated door, blast-resistant utility penetrations - and structure is the element that cannot be retrofitted cheaply. Locating the core early, ideally adjacent to the primary suite for rapid egress, costs a fraction of adding it later.
- **Provide independent, filtered, positive-pressure air,** so that contaminated outside air cannot leak in. Positive pressure holds the room slightly above ambient pressure; air flows out through gaps rather than in. The same system serves wildfire smoke (Category 06) and broader air-quality needs (Category 05).
- **Provide independent power and water** - battery storage sized to ride through an outage, a generator behind it, and a stored water reserve.
- **Locate the data and control systems inside** - server, firewall, air-gapped backup, network core, and security monitoring - so that the systems most needed in a crisis are the best protected during one.
- **Make it survivable, not merely lockable** - a hardened communications path independent of the street, fire-rated data storage, ventilation, and supplies sufficient to wait out a credible event.

> *One hardened room, designed once, that protects the family, the connectivity, the records, and the ability to breathe and function when the rest of the house cannot.*

CATEGORY 05

Biosecurity and Air

This category is included because it has moved from hypothetical to documented, and because the documented cases occurred in ordinary residences. The account that follows is drawn from law-enforcement records and reporting; the related charges are allegations, and the matter remains subject to legal process.

According to a police report and subsequent reporting, in April 2025 a worker who cleaned short-term rentals near Las Vegas entered the garage of a single-family home being rented by the room as an Airbnb and observed household refrigerators, glass beakers of reddish liquid, a biological safety cabinet, and other equipment.[45, 48] The arrest report states that roughly five days after entering, she and another worker became seriously ill; she also reported that other occupants had fallen ill and that one person was hospitalized.[45, 46, 47] On January 31, 2026, the FBI and Las Vegas Metro SWAT, supported by a hazardous-materials team, searched the home and removed refrigerators, containers of unknown liquid, a biosafety hood, and chemicals, which were sent to a federal laboratory for testing.[47, 50]

Investigators traced ownership of the home to a shell company associated with Jia Bei Zhu - also known as Jesse Zhu - a Chinese national who was already in federal custody at the time, and who is alleged to have been connected to an earlier unlicensed laboratory discovered in Reedley, California.[47, 50] Reporting indicates that he allegedly continued to direct the Las Vegas site by telephone, with phone records reflecting roughly 467 calls to the property manager over a year.[46] The property manager was arrested on a felony charge related to hazardous-waste handling.[45] These are allegations that have not been adjudicated.

> **~20**
>
> **INFECTIOUS AGENTS CATALOGUED AT THE REEDLEY SITE BY A CONGRESSIONAL INQUIRY**
>
> Investigators also documented roughly 1,000 genetically engineered mice and a freezer labeled "Ebola" in a populated area.[31, 32]

The Reedley case is documented in a bipartisan congressional investigation. In December 2022, a code-enforcement officer in the Central Valley city investigated a warehouse that was supposed to be vacant; the subsequent inquiry catalogued roughly a thousand genetically engineered mice, approximately twenty infectious agents (including HIV, tuberculosis, and a severe form of malaria), and a freezer labeled "Ebola."[31, 32] The committee found that gaps in federal law had allowed the operation to function undetected, and reporting indicates that initial requests for federal assistance were declined before a member of Congress forced a response.[31, 33]

A 2024 study in The Lancet counted 309 laboratory-acquired human infections worldwide between 2000 and 2021, eight of them fatal - and those occurred in regulated laboratories.[42] Congress treated the pattern seriously enough that the 2026 defense authorization act directed the intelligence community to assess foreign-adversary biotechnology activity.[32] Two laboratories operating from American residences, both shut down within recent years, constitute a documented baseline rather than a hypothetical.

In fairness to the record, when the FBI discussed the Las Vegas case again in March 2026, it stated that the recovered materials largely matched the test-kit business the operators claimed to run and that it identified no confirmed public-health threat.[49] The same statement also noted that the materials had degraded enough to prevent a complete assessment, that influenza components including live virus were present, and that there was no legitimate reason for a private residence to contain such materials.[49] The reassurance concerns intent and findings; the reported illnesses occurred regardless.

Separately, the firms developing frontier AI have issued unusually direct warnings about their own products. When Anthropic released Claude Opus 4 in May 2025, it activated its strictest safety tier specifically to limit assistance with chemical or biological weapons, and reported that expert-graded testing found the unconstrained model could give a novice meaningfully more help than a conventional web search.[24, 25] OpenAI has stated in writing that it expects forthcoming models to reach "High" biological capability and that it is developing safeguards ahead of that threshold.[26, 27] An analysis by the Center for Strategic and International Studies found that both companies moved, within roughly two

years, from reporting little uplift to flagging substantial concern.[27]Anthropic's chief executive has testified to the U.S. Senate that AI could become a "grave threat" by enabling biological misuse, describing it as a medium-term risk rather than science fiction.[53]In June 2026, Anthropic reported substantial progress toward AI systems that accelerate their own development - recursive self-improvement - and stated that effectively slowing the technology to give more time for safety "would likely be a good thing," while stressing that any such slowdown would need to be globally coordinated and verifiable rather than unilateral.[51]Its broader frontier-safety program sets out parallel work on security, safeguards, alignment, and oversight.[52]This is a case for a coordinated option to slow or pause, not a prediction of catastrophe.

The relevant context is that the synthesis barrier was already low before AI. In 2017-2018, a university team reconstructed horsepox - a relative of the eradicated smallpox virus - from mail-order DNA fragments in roughly six months for about $100,000, and published the method; the work was legitimate vaccine research, which is precisely why a leading biosecurity scholar warned that publication lowered the bar for others.[28, 29, 30]AI primarily affects the other input - the expertise and troubleshooting that previously required a specialist. This evidence does not imply that an individual can readily produce a pandemic pathogen. It does imply three separately documented facts: the technical barrier is falling, the manufacturers of the relevant technology are publicly concerned, and unlicensed laboratories have already appeared in residential settings.

> *The design response to this category is not fear; it is filtered air. The same sealed, positive-pressure core specified for protection gives a household one space it can retreat to and breathe in during any airborne event, whatever the source.*

DESIGN IMPLICATIONS

Built into the design, clean-air capability is a small line item with substantial option value: one sealed, positive-pressure space - the protected core of Category 04 - addresses wildfire smoke, an industrial release, a public-health event, or residential contamination with the same system. For a home intended to stand for decades, this has shifted from exotic to basic.

CATEGORY 06

Resilience

A beautiful home is built to be admired; a resilient home is built to keep functioning when conditions stop cooperating. In a crisis, only the second property matters, and January 2025 made the distinction concrete.

When the Palisades and Eaton fires moved through Los Angeles County beginning January 7, 2025, they killed roughly 30 people and destroyed an estimated 16,000 to 18,000 structures.[36]In Pacific Palisades - among the most expensive residential real estate in the country - 56% of structures were leveled, and

estimated real-estate losses exceeded $30 billion.[34]These were not inexpensively built houses; they were destroyed regardless, because finish quality is not a fire rating.

The aftermath also contains the clearest argument for resilient design: repeated images of a home reduced to ash beside a home left standing, on the same street, in the same wind.[34]That outcome was not random. Surviving structures tended to share unglamorous traits - ember-resistant roofing and venting, non-combustible cladding, tempered glazing, defensible space cleared of fuel, and mechanical systems that did not draw burning air inside. The fire was indifferent to square footage and finish budget; it was not indifferent to engineering. Survival did not guarantee habitability, either: a year later, fewer than a dozen destroyed homes had been rebuilt, and many that survived were uninhabitable because of smoke contamination.[34, 35]

> **56%**
>
> **STRUCTURES LEVELED IN PACIFIC PALISADES (JANUARY 2025)**
>
> Estimated real-estate losses exceeded $30 billion; a year later, fewer than a dozen destroyed homes had been rebuilt.[34, 35]

Resilience extends beyond fire to the range of failures a multi-decade asset will eventually meet:

- **Air contamination.** Wildfire smoke, industrial events, and the air-quality concerns of Category 05 point to one capability: the home should be able to seal and filter at least its core spaces and run them on clean, positive-pressure air.
- **Power outages.** Battery storage with generation behind it and the ability to shed non-essential loads keeps refrigeration, medical equipment, communications, security, and air handling running while the grid is down.
- **Communications failures.** When the street connection is cut - by a crew, a fire, or an accident - the home should retain an independent path to the outside world.
- **Broader disruption.** The same protected core, hardened shell, independent utilities, and controlled access that defend against intrusion also carry a household through periods when ordinary services are interrupted.

> *Resilience is invisible until the day it is the only thing that matters. The systems that deliver it are the same ones that deliver security and privacy - one decision, made at design, not three separate budgets.*

SECTION 03

From Research to Evaluation: NES Certified™

The preceding evidence supports a practical conclusion: the qualities that distinguish a resilient high-value residence can be specified, asked about, and evaluated. The 52-question framework in this white paper forms the public basis for NES Certified™, the Institute's AI-Era Residential Resilience Certification. NES Certified™ evaluates high-value residences against a structured framework covering privacy, physical security, cybersecurity, smart-home architecture, the protected core, clean-air capability, power and communications continuity, environmental resilience, and vendor/staff access governance.

The 52-Point AI-Era Residential Resilience Framework organizes the 52 questions into six categories that correspond to the evidence in this paper:

	Category	Questions	Items
A	Site, Perimeter & Physical Security	1-12	12
B	Privacy & Aerial Exposure	13-20	8
C	Network & Cybersecurity	21-32	12
D	The Protected Core	33-41	9
E	Biosecurity & Air	42-45	4
F	Resilience	46-52	7
	Total	**1-52**	**52**

Each of the 52 questions is scored from 0 to 3 under a proprietary rubric:

- **0** - Not Addressed
- **1** - Minimally Addressed
- **2** - Sufficiently Addressed
- **3** - Exemplary

The maximum raw score is 156 points. The certification designation is based on total score, category performance, documentation quality, and critical-gating rules designed so that a strong average cannot

mask a critical deficiency in an essential area. The detailed scoring rubric, weighting, evaluator guidance, and gating methodology are proprietary to The New Estate Standard Institute.

0-156

RAW SCORE RANGE · 52 QUESTIONS SCORED 0-3

The certification designation reflects total score, category-level performance, documentation quality, and critical-gating rules. The detailed rubric is proprietary and is not a measure of guaranteed safety.

NES Certified™ evaluates how well a residence aligns with this framework. It does not guarantee safety, security, code compliance, insurance acceptance, or threat prevention, and it does not certify that a home is secure. NES Certified™ is not a guarantee of safety or threat prevention; it is a quantitative, documentation-supported evaluation of framework alignment.

> *Certification measures alignment with a standard. It does not - and cannot - guarantee an outcome.*

SECTION 04

Why Design Timing Matters

The evidence in this paper is industry-agnostic, and a growing number of builders, architects, and security consultants now treat security, privacy, data, and resilience as architecture rather than accessories. The purpose of this short section is narrower: to make one point about when these problems are solved, because timing is where most homes fail the test.

A reinforced protected core, a hardwired and segmented network backbone, filtered positive-pressure air, independent power and water, screened sightlines, and a perimeter that accounts for the back of the lot are inexpensive as lines on a drawing and expensive - or impossible - as retrofits. Built in during design, their cost is a rounding error against the cost of the house. Added later, the cost is measured in demolition, or in the event that was not planned for.

> *Structure, sightlines, network backbone, and a protected core are decided with a pencil. They are the questions that must be asked before the slab is poured.*

The underlying principle is simple to state and harder to practice: decide what must survive - the family first, then connectivity, records, and the ability to breathe and function - and design outward from that core, rather than finishing a beautiful house and assuming conditions will never test it. Understood this way, resilience and security are not a separate budget added to luxury; they are part of what the word should now mean - that a home is not only beautiful, but will still be standing, still functioning, and still safe on the day that matters.

INQUIRY

An Invitation to Inquiry

This paper is intended as a research foundation, not a sales document. Readers evaluating, designing, or advising on high-value residences are encouraged to use it as a basis for inquiry. To go deeper:

- **Download the 52-question buyer guide** - the checklist in Appendix A, formatted for use with an architect, builder, security consultant, or agent.
- **Request the NES Certified™ Applicant Overview** - a description of the evaluation process and the documentation an assessment requires.
- **Request a private property evaluation** - a confidential, framework-based assessment of a specific residence.
- **Contact The New Estate Standard Institute LLC** - for research inquiries, briefings, or questions about the framework.

The New Estate Standard Institute can be reached at newestatestandard.com. Inquiries are treated as confidential, and nothing in this paper is an offer to sell, or a solicitation to buy, any property or security.

LEGAL

Important Disclaimer

This white paper is educational and informational. It does not provide legal, security, cybersecurity, engineering, insurance, HVAC, fire, medical, or other professional advice, and it should not be relied upon as a substitute for qualified professionals retained for a specific property and circumstance. No home can be guaranteed safe, secure, immune from attack, or protected against all risks; the measures described reduce certain exposures but cannot eliminate risk.

Statements in this paper are drawn from public reporting, government and primary sources, and expert commentary as cited. Matters described as alleged, suspected, or charged refer to claims that are the subject of investigation or legal process and have not been adjudicated; nothing here should be read as a determination of guilt. Forward-looking statements are reasoned inferences from documented trends, not predictions of future events.

NES Certified™ evaluates framework alignment. It does not guarantee safety, security, code compliance, insurance acceptance, or threat prevention, and certification does not represent that a home is secure. NES Certified™ is a trademark of The New Estate Standard Institute LLC; other trademarks and source names referenced in this paper belong to their respective owners.

SOURCES

References

Sources are listed in the order first cited. Government and primary sources are preferred; reported allegations are attributed to the outlets that reported them.

1. ABC News, “FBI issues warning about burglaries of pro athletes’ homes” (Dec. 2024). https://abcnews.go.com/US/fbi-issues-warning-burglaries-pro-athletes-homes/story?id=117197676
2. ESPN, “FBI warns leagues about targeted burglaries of athletes’ homes” (Dec. 2024). https://www.espn.com/espn/story/_/id/43227536/fbi-warns-leagues-targeted-burglaries-athletes-homes
3. CNN, “Professional athletes’ homes are still getting broken into. Here’s how the FBI says the thieves operate” (Jan. 2025). https://www.cnn.com/2025/01/11/us/professional-athlete-break-ins-fbi
4. FBI Los Angeles Field Office, “Valuable Items Stolen During Los Angeles Burglaries by South American Theft Groups Found in Chile and Returned to Victims, Including Actor Keanu Reeves” (Nov. 2025). https://www.fbi.gov/contact-us/field-offices/losangeles/news/valuable-items-stolen-during-los-angeles-burglaries-by-south-american-theft-groups-found-in-chile-and-returned-to-victims-including-actor-keanu-reeves-
5. CNN, “‘They hit the jackpot’: How so-called ‘burglary tourists’ use visa waivers to target luxury US homes” (Apr. 2024). https://www.cnn.com/2024/04/05/us/burglary-tourists-visa-waivers-target-luxury-homes
6. CBS Los Angeles, “California ‘crime tourism’ ring worked with South American theft groups and laundered millions, prosecutors say” (Aug. 2024). https://www.cbsnews.com/losangeles/news/crime-tourism-ring-in-socal-worked-with-south-american-theft-groups-and-laundered-millions-prosecutors-say/
7. 12News (KPNX), “Luxury homes in Scottsdale targeted by burglars” (2024). https://www.12news.com/article/news/crime/scottsdale-break-ins-tied-to-south-american-crime-ring/75-0b7df4b0-f5f3-47cc-811f-486e0c9c5144
8. AZFamily (3TV/CBS 5), “Scottsdale Police arrest 3 members of a South American crime group linked to dinner-time burglaries” (Mar. 2024). https://www.azfamily.com/2024/03/12/scottsdale-police-arrest-3-people-burglaries-connected-south-american-organized-crime/
9. Ahwatukee Foothills News, “Scottsdale frets over Chilean ‘tourist burglars’” (Mar. 2024). https://www.ahwatukee.com/news/scottsdale-frets-over-chilean-tourist-burglars/article_95e1fedc-da78-11ee-bfac-3bcd1b283285.html
10. Fox News, “‘Burglary tourism’ plagues Southern California as unvetted foreigners raid luxe houses” (Mar. 2024). https://www.foxnews.com/us/burglary-tourism-plagues-southern-california-unvetted-foreigners-raid-luxe-houses
11. Fox News / Fox 11, report on Colombian nationals arrested in a Southern California burglary-tourism ring (camouflaged surveillance devices). https://www.foxnews.com/us
12. United States v. Causby, 328 U.S. 256 (1946), via FindLaw. https://caselaw.findlaw.com/court/us-supreme-court/328/256.html
13. UAV Coach, “Can You Fly a Drone Over Private Property?” (2026 update). https://uavcoach.com/drone-over-private-property/
14. Bolt Flight, “Can You Shoot Down a Drone Over Your Property? FAA Rules & Airspace Rights” - 18 U.S.C. § 32 (Nov. 2025). https://boltflight.com/can-you-shoot-down-a-drone-over-your-property-faa-rules-airspace-rights/
15. Legal Overview, “Is It Illegal to Shoot Down a Drone in 2026?” - FCC jamming prohibition, 47 U.S.C. § 333. https://legaloverview.com/is-it-illegal-to-shoot-down-a-drone-in-2026/

16. FBI, “FBI Releases Annual Internet Crime Report” (Apr. 2025) - $16.6B, +33%. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

17. FBI Internet Crime Complaint Center, 2024 Internet Crime Report (PDF). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

18. Anthropic, “Disrupting the first reported AI-orchestrated cyber espionage campaign” (Nov. 2025). https://www.anthropic.com/news/disrupting-AI-espionage

19. Anthropic, full technical report on the GTG-1002 campaign (PDF, Nov. 2025). https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf

20. FBI/CNMF/NSA & CISA Joint Cybersecurity Advisory, “People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations” (Sept. 2024, PDF). https://www.ic3.gov/CSA/2024/240918.pdf

21. CISA, “Heightened DDoS Threat Posed by Mirai and Other Botnets” (2016). https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

22. U.S. Department of Justice, “Court-Authorized Operation Disrupts Worldwide Botnet Used by People’s Republic of China State-Sponsored Hackers” (Sept. 2024). https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

23. FBI Public Service Announcement, “Home Internet Connected Devices Facilitate Criminal Activity” (BADBOX 2.0, June 2025). https://www.fbi.gov/investigate/cyber/alerts/2025/home-internet-connected-devices-facilitate-criminal-activity

24. Anthropic, “Activating AI Safety Level 3 Protections” (May 2025). https://www.anthropic.com/news/activating-asl3-protections

25. TIME, “Exclusive: New Claude Model Triggers Safeguards at Anthropic” (May 2025). https://time.com/7287806/anthropic-claude-4-opus-safety-bio-risk/

26. Fortune, “OpenAI warns its future models will have a higher risk of aiding bioweapons development” (June 2025). https://www.fortune.com/2025/06/19/openai-future-models-higher-risk-aiding-bioweapons-creation

27. Center for Strategic and International Studies (CSIS), “Opportunities to Strengthen U.S. Biosecurity from AI-Enabled Bioterrorism: What Policymakers Should Know.” https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should

28. Science (AAAS), “A paper showing how to make a smallpox cousin just got published. Critics wonder why” (Jan. 2018). https://www.science.org/content/article/paper-showing-how-make-smallpox-cousin-just-got-published-critics-wonder-why

29. Johns Hopkins University Hub, “Scientists bring back extinct horsepox virus in lab, raising important biosecurity questions” (Jul. 2017). https://hub.jhu.edu/2017/07/11/horsepox-virus-recreated-lab-canada/

30. F. E. Sharples, “Synthesis of Horsepox from Mail-Order DNA,” Applied Biosafety (2017). https://journals.sagepub.com/doi/full/10.1177/1535676017724433

31. U.S. House Select Committee on the Chinese Communist Party, Investigation into the Reedley Biolab (report, Nov. 2023, PDF). https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/scc-reedley-report-11.15.pdf

32. Lawfare, “Two Illegal Biolabs Reveal Gaps in U.S. Biosecurity.” https://www.lawfaremedia.org/article/two-illegal-biolabs-reveal-gaps-in-u.s.-biosecurity

33. KVPR, “House committee releases report on illegal Reedley biolab” (Nov. 2023). https://www.kvpr.org/local-news/2023-11-15/congressional-committee-completes-report-into-illegal-reedley-medical-lab

34. KTLA, “Report: Real estate losses from the Palisades, Eaton wildfires could top $30 billion” (Feb. 2025). https://ktla.com/news/local-news/report-real-estate-losses-from-the-palisades-eaton-wildfires-could-top-30-billion/

35. NBC News, “A year after L.A.-area wildfires destroyed thousands of homes, fewer than a dozen have been rebuilt” (Jan. 2026). https://www.nbcnews.com/news/us-news/year-la-area-wildfires-destroyed-thousands-homes-fewer-dozen-rebuilt-rcna252751

36. FOX Weather, “Recounting the heartbreaking loss caused by the deadly Palisades and Eaton fires 1 year later” (Jan. 2026). https://www.foxweather.com/extreme-weather/palisades-eaton-california-los-angeles-county-wildfires-one-year-later

37. Atomic Heritage Foundation / National Museum of Nuclear Science & History, “Greenbrier Bunker.” https://ahf.nuclearmuseum.org/ahf/history/greenbrier-bunker/

38. The Philadelphia Inquirer (Michael Smerconish), “Touring the secret Cold War bunker that Congress never used” (Aug. 2018). https://www.inquirer.com/philly/columnists/michael_smerconish/greenbrier-bunker-west-virginia-congress-20180802.html

39. Wikipedia, “Project Greek Island” (Greenbrier continuity-of-government facility). https://en.wikipedia.org/wiki/Project_Greek_Island

40. FEMA, “Safe Room Publications and Resources” - FEMA P-361, P-320, and ICC 500. https://www.fema.gov/emergency-managers/risk-management/building-science/safe-rooms/resources

41. National Storm Shelter Association, “Residential Tornado Shelters” - near-absolute protection, 250 mph design. https://www.nssa.cc/residential-tornado-shelters.html

42. The Lancet (2024), study counting 309 laboratory-acquired human infections worldwide (2000-2021), eight deaths; summarized in The Maha Report investigation of the Reedley lab. https://www.themahareport.com/p/exclusive-how-a-california-code-enforcement

43. FBI, 2024 Cyber Alerts index - Volt Typhoon and SOHO router compromise; risk from Chinese-manufactured drones to critical infrastructure. https://www.fbi.gov/investigate/cyber/alerts/2024

44. Paul, Weiss, “Anthropic Disrupts First Documented Case of Large-Scale AI-Orchestrated Cyberattack” - including prior North Korean IT-worker misuse (Nov. 2025). https://www.paulweiss.com/insights/client-memos/anthropic-disrupts-first-documented-case-of-large-scale-ai-orchestrated-cyberattack

45. Las Vegas Review-Journal, “Man arrested in Las Vegas bio lab case appears in federal court” - police-report detail on ~5-day onset and hospitalization (Feb. 2026). https://www.reviewjournal.com/crime/courts/man-arrested-in-las-vegas-bio-lab-case-appears-in-federal-court-3615544/

46. KTNV (Channel 13, Las Vegas), “Police source describes falling ‘deathly ill’ after entering garage where illegal lab was found” - April 2025 exposure, ~467 jail calls (Feb. 2026). https://www.ktnv.com/news/crime/police-source-describes-falling-deathly-ill-after-entering-garage-where-illegal-lab-was-found

47. The Hill, “What to know about suspected biolab in Las Vegas” - Airbnb operation, pathogen-labeled containers, illnesses (Feb. 2026). https://thehill.com/homenews/state-watch/5722839-hazardous-waste-seized-vegas/

48. ABC News, “Housecleaner said multiple illnesses tied to Las Vegas house with possible bio lab: Police report” (Feb. 2026). https://abcnews.go.com/US/housecleaner-multiple-illnesses-tied-las-vegas-house-bio/story?id=129865238

49. GV Wire, “FBI Reveals Contents of Las Vegas Biolab” - degraded materials, influenza components, no legitimate reason for a residence to hold them (Mar. 2026). https://gvwire.com/2026/03/16/fbi-reveals-contents-of-las-vegas-biolab-nothing-too-crazy-they-say/

50. Vision Times, “FBI Raids Las Vegas Home, Uncovers Illegal Biolab Linked to China” - residential home, garage lab, raid of Jan. 31, 2026, LLC ownership traced to Jia Bei Zhu (Feb. 2026). https://www.visiontimes.com/2026/02/04/fbi-raids-las-vegas-home-uncovers-illegal-biolab-linked-to-china.html

51. Anthropic Institute, “When AI builds itself: Our progress toward recursive self-improvement, and its implications” (June 2026). https://www.anthropic.com/institute/recursive-self-improvement

52. Anthropic, "Frontier Safety Roadmap" (updated 2026). https://www.anthropic.com/responsible-scaling-policy/roadmap

53. Dario Amodei, "Written Testimony of Dario Amodei, Ph.D., Co-Founder and CEO, Anthropic," hearing on "Oversight of A.I.: Principles for Regulation," U.S. Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law (July 25, 2023). https://www.judiciary.senate.gov/imo/media/doc/2023-07-26_-_testimony_-_amodei.pdf

Primary source categories

- **Government & primary** - FBI annual Internet Crime Report and IC3 advisories; FBI Los Angeles Field Office; U.S. Department of Justice botnet takedown; CISA/NSA joint advisories and the Mirai alert; U.S. House Select Committee on the CCP (Reedley); FEMA safe-room guidance and ICC 500; United States v. Causby (U.S. Supreme Court).
- **Academic & scientific** - Science (AAAS) and Johns Hopkins commentary on horsepox synthesis; Applied Biosafety; The Lancet (2024) laboratory-acquired infections study; CSIS analysis of AI-enabled biosecurity risk.
- **Industry & primary disclosures** - Anthropic safety and incident disclosures; OpenAI Preparedness Framework as reported and analyzed; National Storm Shelter Association shelter standards.
- **News reporting** - ABC News, CNN, CBS News, ESPN (athlete and luxury-home burglaries); 12News, AZFamily, Ahwatukee Foothills News, Fox News (Arizona "Dinnertime" burglaries); KTLA, FOX Weather, NBC News (Palisades and Eaton fires); Las Vegas Review-Journal, KTNV, The Hill, GV Wire, Vision Times (residential biolab reporting); TIME (AI safety).

Further reading

- FBI Internet Crime Complaint Center (ic3.gov) - file a complaint and review current advisories.
- CISA "Secure Our World" and IoT security guidance - a practical baseline for home-network defense.
- NIST Cybersecurity Framework and consumer-IoT guidance (NIST IR 8259 series) - standards a security consultant should know.
- FEMA Building Science safe-room library - design references for a protected core.
- Johns Hopkins Center for Health Security - ongoing biosecurity analysis and commentary.

APPENDIX A

The 52 Questions Every Luxury Home Buyer, Builder, or Advisor Should Ask

These 52 questions are the public basis of the NES Certified™ framework. They are written to be asked of an architect, builder, security consultant, or agent. Where a question cannot be answered, that absence is itself informative.

A Site, Perimeter & Physical Security

1. What is the true physical perimeter of the property, including washes, golf-course frontage, easements, and service alleys, and what barrier, detection, and lighting secures each approach?
2. Can someone reach the back of the lot or the house without passing the front gate? If so, how is that path controlled?
3. Are exterior cameras and alarm components hardwired, and do they store and verify footage locally?
4. What happens to the security system if Wi-Fi is jammed from the street: does it fail safe or fail blind?
5. Is there a true safe room built to FEMA P-361 / ICC 500 standards, or just a reinforced closet?
6. Is the protected space reachable from the primary suite by a short, direct path within the same secured zone, without crossing exterior or publicly exposed areas?
7. Are sightlines into the most-used private spaces screened from public vantage points and from low airspace?
8. Does the landscaping create concealment for someone surveilling or waiting, such as dense beds against the house or unlit zones?
9. Is there exterior lighting and motion detection covering every approach, including the roofline?
10. Does the property have controlled service and delivery access infrastructure, such as a separate service entry, video or intercom at entry points, access-controlled gates or locks, and electronic access-logging capability?
11. Can the interior layout and high-value rooms be seen or inferred from publicly accessible vantage points, such as the street, sidewalk, a shared drive, or a neighboring elevation, through unscreened glazing?
12. Does the security system support monitored alarm signaling with distinct armed-stay and armed-away modes, separately zoned interior and perimeter detection, and duress or panic signaling?

B Privacy & Aerial Exposure

13. From the cone of airspace a drone can legally occupy, which interior and exterior spaces are visible?
14. How does the design baffle aerial sightlines into the primary suite, pool, and glass-walled rooms?
15. Are outdoor living areas placed where they can be observed from above, and can they be relocated or screened?
16. Does the property include at least one open-air space, such as a courtyard, atrium, or screened terrace, usable for private outdoor living without exposure to street or overhead observation?
17. What glazing and window-treatment strategy protects rooms that face open sky?
18. Is there drone-detection capability appropriate to the property, given that interdiction is unlawful for private owners?
19. Are interior-facing cameras, microphones, and voice assistants positioned, and the system architected, so that private interior spaces are not wired or configured to continuously record or stream to third-party cloud services?
20. Are the motor court, garage, and vehicle movements screened from street-level and overhead observation, so arrivals, departures, and vehicle inventory cannot be easily catalogued?

C Network & Cybersecurity

21. Is the home wired with structured cabling, with Wi-Fi reserved for convenience rather than the security layer?
22. Are the family's devices, the security system, and smart-home devices on separate, isolated network segments, such as VLANs?
23. Is there a dedicated, business-grade hardware firewall, not the internet provider's default router?
24. Do connected devices reject known default credentials, with none left on factory defaults, and is a current device-and-firmware inventory kept with the property?
25. How is remote access to home systems handled: through an encrypted VPN into a controlled entry point, or through scattered cloud apps?
26. Where do the smart-home platforms send data, and which are cloud-dependent in ways that fail when connectivity drops?
27. Does the access-control and identity configuration enforce unique per-vendor and per-integrator accounts, least-privilege roles, multi-factor authentication, and access logging?
28. Does the home's access and admin configuration show any standing "master", installer, or default administrative accounts, or always-on vendor remote-access tunnels, rather than only per-user, revocable accounts?
29. Is there an encrypted, air-gapped backup of irreplaceable data, physically disconnected from any network?

30. Is complete, current system documentation resident with the property, such as network as-builts, security and smart-home configuration records, and a credential register, sufficient for any qualified party to maintain the home's systems over time?
31. Are the home's networked devices, such as cameras, NAS, and routers, current vendor-supported models still receiving security updates, rather than end-of-life or unsupported models?
32. Does the network architecture support rapid containment, the ability to isolate or quarantine a compromised device or segment without disabling the whole home, with logging to support investigation?

D The Protected Core

33. Does the design include a single hardened core that combines safe room, server/communications room, data vault, and shelter?
34. What is the shell, reinforced concrete or CMU, and is the door vault-rated?
35. Does the core have a filtered, positive-pressure air system independent of the main HVAC?
36. Does the core have independent power, such as battery plus generator, sized to ride through a multi-day outage?
37. Is there a stored potable-water reserve sized for the protected space's design occupancy and intended duration?
38. Are the network's heart, firewall, air-gapped backup, and security monitoring located inside the hardened shell?
39. Does the protected core retain a hardened, last-resort communications path within the shell that does not depend on the street cable or street utilities?
40. Is the data storage in the core fire-rated, ideally fireproof?
41. Is the protected core structurally integrated into the building, with an engineered shell, load paths, and utility penetrations that are part of the structure, rather than a non-structural enclosure fitted into finished space?

E Biosecurity & Air

42. Can at least one core space be sealed and run on filtered, positive-pressure air during an airborne event?
43. What grade of filtration does the clean-air system use, and is it built with accessible, serviceable filter stages and condition monitoring, such as differential-pressure indication?
44. How is fresh-air intake positioned and protected relative to the street, mechanical equipment, and prevailing wind?
45. Is the clean-air capability integrated with the protected core, so one system serves smoke, contamination, and shelter needs?

F Resilience

46. Is the home built with ember-resistant roofing and venting, non-combustible cladding, and tempered glazing?
47. Is there genuine defensible space, and is landscaping specified to reduce fuel near the structure?
48. How long can the home sustain refrigeration, medical equipment, communications, security, and air handling during a grid outage?
49. Does the whole home retain an independent communications path for continuity if local infrastructure fails?
50. Does the design limit post-event smoke and contamination persistence, through compartment sealing, filterable or ductable spaces, and cleanable, non-porous interior materials?
51. Are the resilience, security, and privacy systems physically coordinated, sharing the protected core, backup power, and communications, with non-conflicting layouts, rather than independent systems with redundant or conflicting infrastructure?
52. Does the construction show security and resilience built in natively, such as concealed conduit and cabling and dedicated mechanical and electrical capacity, rather than surface-mounted or retrofitted additions?

ABOUT

About The New Estate Standard Institute LLC

The New Estate Standard Institute LLC is a private research, education, evaluation, and certification initiative focused on AI-era residential resilience for high-value homes. The Institute develops frameworks, buyer guidance, technical research, and evaluation tools for privacy, physical security, cyber resilience, smart-home architecture, clean-air capability, protected infrastructure, backup power, communications continuity, environmental resilience, and vendor/staff access governance.

The Institute's central thesis is simple: safety standards change when the environment changes. Seat belts, fire systems, smart locks, doorbell cameras, hurricane glass, protected rooms, and residential cybersecurity all reflect the same pattern. As the AI era changes the risk environment around high-value residences, buyers, builders, advisors, and agents need better questions, better documentation, and better evaluation frameworks.

DOCUMENT INFORMATION

Title: Luxury Homes in the Era of AI - A Technical White Paper on Privacy, Security, Cyber Resilience, Clean Air, Protected Infrastructure, and Continuity for High-Value Residences.

Published by The New Estate Standard Institute LLC. Certification: NES Certified™ - AI-Era Residential Resilience Certification. Framework: The 52-Point AI-Era Residential Resilience Framework. Version 1.0 · 2026.

This document is educational and informational and does not constitute professional advice. See the Publisher Note and full disclaimer for details.