NIST SP 800-53 Control Mapping

Windows Hardening Baseline

Mapping of the curated Windows configuration baseline to the security and privacy control objectives of NIST SP 800-53.

Project	briangeis/windows-hardening
Framework	NIST SP 800-53 Revision 5, Release 5.2.0
Baseline	Policy-Windows-Base.psd1 and Policy-Windows-NoStoreApps.psd1
Target	Windows 11 25H2, standalone and not joined to a domain
Settings	134 (112 base, 22 layer)
Author	Brian Geis, briangeis.com/samples
Version	1.3
Reviewed	2026-09-23

Contents

1. Executive Summary....3
2. Purpose, Scope, and Claims....4
    2.1 Purpose....4
    2.2 Scope....4
    2.3 Claims and Limitations....4
    2.4 Method....5
3. System Description....5
    3.1 Target System....5
    3.2 Control Inheritance....6
    3.3 Enforcement Mechanism....6
    3.4 Artifact-Level Contributions....7
4. Control Mapping....8
    4.1 Telemetry and Diagnostics....8
    4.2 Microsoft Cloud Services....8
    4.3 App Permissions....9
    4.4 Windows Features....10
    4.5 Windows Update....10

4.6 Internet Explorer....11
4.7 Background Services....11
4.8 Telemetry and Reporting....12
4.9 Security Defaults....12
4.10 Activity and History....12
4.11 Content Delivery....13
4.12 Windows Applications....13
5. Control Narratives....13
5.1 PT-3, Personally Identifiable Information Processing Purposes....14
5.2 CM-7, Least Functionality....14
5.3 SC-7, Boundary Protection....15
5.4 SI-12, Information Management and Retention....16
5.5 AC-20, Use of External Systems....16
5.6 MP-7, Media Use....17
5.7 SC-15 and SC-42, Collaborative Computing and Sensor Data....17
5.8 AC-11, IA-5, and IA-11, Device Lock and Authentication....18
5.9 SC-28, Protection of Information at Rest....19
5.10 CM-3 and CM-6, Change Control and Configuration Settings....19
6. Coverage Analysis....20
6.1 Control Origination....20
6.2 Scoping Considerations....21
6.3 Controls Not Addressed....23
7. Where the Baseline Works Against a Control Objective....23
7.1 Defender Cloud Protection....24
7.2 SmartScreen for Store Apps and Internet Explorer....24
7.3 Find My Device....24
7.4 Store Application Updates....25
8. Settings the Baseline Declines....25
8.1 Windows Update....26
8.2 Time Synchronization and Trust Anchors....27
9. Notes for Assessors....27
10. Traceability....28
11. References....29
12. Revision History....30

1. Executive Summary

The curated Windows baseline applies 134 configuration settings to a standalone Windows device: 112 in the base profile and 22 in the optional No Store Apps layer. This document maps each to the NIST SP 800-53 control objectives it advances, with the largest concentrations in personally identifiable information processing purposes (PT-3), least functionality (CM-7), and boundary protection (SC-7). Four findings bear on how that coverage should be read.

Only 25 of the 134 assignments are against controls a system implements on its own. NIST marks 64 organization-implemented, including all 38 for PT-3 and all 10 for SI-12, and the remaining 45 both. A device configuration can support those objectives and can never satisfy them alone. Any assessment crediting this baseline needs the organizational half supplied separately, and Section 6.1 gives the split for every control cited.

Twenty-one settings do not take effect on a current Windows 11 device. The baseline serves Windows 10 and Windows 11 from one profile deliberately, so it carries settings that take no effect on newer builds, and others conditional on hardware or licensing. Coverage should be read against the configuration being assessed rather than the count applied. The conditions are enumerated per setting in Section 6.2.

Enforcement differs by Windows edition, and the difference is substantial. On Pro and higher, 123 of the 134 settings are written to Local Group Policy and re-applied at every policy refresh, so a manual change is reverted. On Home, and for the 11 settings that fall outside the policy branches on any edition, the write happens once and nothing re-asserts it. Section 3.3 and Section 9 set out what each case does and does not demonstrate.

Six settings improve one control objective at the cost of another, and 28 catalog settings are declined rather than applied. Both sets are deliberate and both are recorded with the reasoning, in Section 7 and Section 8. Each exclusion names the control objective it protects, and the declined set includes every setting that would break clock synchronization, certificate trust, or security patching, none of which this baseline trades for privacy.

Taken together, the baseline is a device-layer contribution to a control program rather than a substitute for one. It does what device configuration can do, and records where that ends.

2. Purpose, Scope, and Claims

2.1 Purpose

This document maps each setting in the curated Windows configuration baseline to the NIST SP 800-53 control objectives it advances, so that a system owner or assessor can determine which objectives the baseline supports, which it leaves unaddressed, and which it affects adversely.

It is read alongside profiles/reference/Policy-Windows.md, which records the editorial reasoning behind the curation. That document addresses what to apply and why. This one addresses what the result contributes against a control framework.

2.2 Scope

In scope are the 134 settings carried by the two curated profiles: 112 in the base and 22 in the No Store Apps layer.

Four things are out of scope. The settings cataloged in the definitions files but not curated into either profile appear in Section 8 as declined rather than as coverage. The Microsoft Edge target is hardened separately. Windows services and preinstalled package removal are the concern of other components. And any control objective requiring organizational process rather than device configuration falls outside what this document can address at all.

The distinction between the catalog and the baseline matters and is easy to lose. The definitions files catalog what can be configured. The curated profiles record what to apply. A coverage claim can only be made about a configuration that is actually applied, so the subject of this document is the profiles.

2.3 Claims and Limitations

This document makes a deliberately narrow claim.

It asserts that applying a given setting advances the stated control objective on the target device, and identifies where a setting advances only part of an objective or advances it incidentally.

It does not assert that the baseline satisfies any control, that a device applying the baseline is compliant with any framework, or that this mapping constitutes an assessment. It issues no findings. Whether a control is satisfied depends on organizational policy, procedure, monitoring, and evidence that a device configuration cannot supply, and Section 6.1 shows how much of this baseline's contribution is against controls NIST designates as organization-implemented.

The verb throughout is **supports**. A configuration setting contributes to a control objective. It does not satisfy a control. The word *satisfies* appears in this document only in explicit negation.

2.4 Method

Assignments were made by reading the control text and its assessment objectives, not the control titles, against the setting's documented behavior and side effects. The authoritative source was NIST's OSCAL catalog at Release 5.2.0, which carries the current control text, the SP 800-53A assessment objectives, and each control's implementation designation. The published PDF of SP 800-53 Rev. 5 predates Releases 5.1.1 and 5.2.0 and was not used as the control-text source.

This is a **supportive relationship mapping** in the sense of NIST IR 8278A Rev. 1: it records how a supporting concept, a configuration setting, helps achieve a supported concept, a control. The set-theory relationships of the OLIR program do not apply, because a registry setting is not a subset, superset, or equivalent of a control. The strength scale is defined here:

Relationship	Meaning
Supports	Advances the control objective directly and materially
Partially supports	Advances one element of a multi-element objective
Incidental	Advances the objective as a side effect of a different primary purpose

The mapping follows the six mapping principles set out in the compliance mappings overview.

An assignment would be invalidated by a change to the control text in a later release, by a change in the setting's behavior in a later Windows feature update, or by evidence that a setting does not behave as its definitions entry records. The `Reviewed` date above records when the assignments were last checked against both.

3. System Description

3.1 Target System

The baseline targets a standalone device: locally administered, not joined to an Active Directory domain, and receiving no centrally managed policy. Broad Windows 10 compatibility is retained deliberately, and Section 6.2 explains what that costs in coverage terms.

Whether the device is centrally managed is the first compatibility question a reader should settle. The toolkit is intended for personal or business devices not joined to a domain, where domain policy would otherwise take precedence over local policy. `Disable MDM Enrollment` in the base

illustrates the boundary: on an unmanaged device it is least functionality, closing an enrollment path the owner does not use, and on a device an organization intends to manage centrally it obstructs the management channel and the CM-7 reading inverts.

3.2 Control Inheritance

The standalone posture decides which controls are in scope before any individual setting is considered.

A **common control**, in the SP 800-53 glossary, is a control inherited by multiple systems. A domain-joined endpoint inherits identity management, centralized audit collection, policy enforcement, and update management from domain infrastructure. **A standalone device inherits nothing, so it has no common controls available to it and every control is system-specific.** Every objective is met on the device or not at all.

Two consequences follow. Controls in the AU family that depend on forwarding records to a central collector cannot be met by device configuration, so the settings here that limit local diagnostic retention are addressed to data minimization rather than to audit capability. And the mechanism that keeps the baseline in place after it is applied differs by Windows edition, which bears directly on what the evidence in Section 9 can demonstrate. Section 3.3 sets out the difference.

3.3 Enforcement Mechanism

The mechanism by which a setting is applied determines whether it stays applied, and the difference between editions is substantial rather than incidental.

On Home edition, where Local Group Policy is unavailable, the toolkit writes registry values directly. On Pro, Enterprise, Education, and LTSC editions it writes through `LGPO.exe`, which records the settings in Local Group Policy. The Group Policy engine then re-applies them at every policy refresh, by default at startup and on a background interval of roughly 90 minutes. A value that a local administrator changes manually is restored at the next refresh.

That is a continuously operating enforcement mechanism, and it covers most of the baseline:

Registry location	Settings	Behavior after application
Under a `\Policies\` key	123	Managed by Group Policy and re-applied at every refresh on non-Home editions
Outside the `\Policies\` keys	11	Written once and not re-asserted on any edition

The 11 exceptions are settings whose target values do not live under a policy branch, so Group Policy does not manage them even where it applied them: `Disable Fast Startup`, `Disable Advertising ID (Feature)`, `Disable App Launch Tracking`, `Disable Language List Access`, `Disable License Manager Service`, `Disable Microsoft Account Sign-In Assistant`, `Disable OneDrive Network Traffic Before Sign-In`, `Disable SmartScreen for Store Apps`, `Disable ActiveX VersionList Download`, `Set Feedback Period to Zero`, and `Set Feedback Count to Zero`. These behave on every edition the way the whole baseline behaves on Home.

Two consequences follow for an assessment. On non-Home editions a policy artifact exists in Local Group Policy and can be examined directly, and the 123 managed settings are re-asserted rather than merely present. On Home, and for the 11 exceptions everywhere, a setting can be changed by any local administrator and nothing restores it. Section 9 sets out what each case demonstrates as evidence.

Local Group Policy is superseded by domain policy where one exists, so this enforcement holds for the standalone case the baseline targets and not for a device later joined to a domain.

3.4 Artifact-Level Contributions

Some controls are supported by the toolkit's artifacts rather than by any individual setting. These are reported separately and are **not** counted among the 134 setting assignments, because folding a different kind of claim into the setting counts would inflate the coverage figures.

Control	Origination	Artifact and contribution
CM-2 Baseline Configuration	O	The curated profile is a documented, version-controlled configuration baseline for the device. Supports CM-2a
CM-2(3) Retention of Previous Configurations	O	Snapshot Mode captures system state before any change, retaining the prior configuration to support rollback
CM-6 Configuration Settings	O/S	The definitions files are the documented setting catalog, the profiles establish the baseline, the scripts implement it. Supports CM-6a and CM-6b
CM-6 Configuration Settings	O/S	The profile reference documents identify and document 28 deviations from the catalog with reasons. Supports CM-6c. Approval remains organizational
CM-3 Configuration Change Control	O	Snapshot comparison provides the record against which configuration change can be identified. Incidental, and detection is manual on Home. On non-Home editions Group Policy reverts unauthorized change to the 123 managed settings without detection being required

4. Control Mapping

Settings are grouped by their category in the definitions files. `Profile` identifies whether a setting is in the base or in the No Store Apps layer. An asterisk marks a setting subject to a scoping consideration, meaning it does not take effect on every supported configuration. The conditions are enumerated in Section 6.2 and differ from setting to setting.

4.1 Telemetry and Diagnostics

Setting	Profile	Control	Relationship	Also Supports
Set Diagnostic Data to Minimum	Base	PT-3	Supports	-
Disable Tailored Experiences	Base	PT-3	Supports	-
Disable Consumer Experiences	Base	CM-7	Supports	PT-3 (incidental)
Disable Feedback Notifications	Base	CM-7	Supports	PT-3 (incidental)
Set Feedback Period to Zero	Base	CM-7	Partially supports	-
Set Feedback Count to Zero	Base	CM-7	Partially supports	-
Disable Advertising ID (Feature)	Base	PT-3	Supports	-
Disable Advertising ID (Policy)	Base	PT-3	Supports	CM-6 (partially supports)
Disable Language List Access	Base	PT-3	Supports	-
Disable MAPS Reporting	Base	PT-3	Supports	-
Disable Sample Submission	Base	PT-3	Supports	-
Disable MSRT Diagnostic Data	Base	PT-3	Supports	-
Disable Enhanced Notifications	Base	CM-7	Supports	-
Restrict Implicit Text Collection	Base	PT-3	Supports	-
Restrict Implicit Ink Collection	Base	PT-3	Supports	-

4.2 Microsoft Cloud Services

Setting	Profile	Control	Relationship	Also Supports
Disable OneDrive File Storage	Layer	AC-20	Supports	CM-7 (partially supports)
Disable OneDrive Network Traffic Before Sign-In	Layer	SC-7	Supports	-
Disable Microsoft Account Sign-In Assistant	Layer	AC-20	Supports	CM-7 (partially supports)
Disable Web Results in Search	Base	SC-7	Supports	PT-3 (partially supports)
Disable Web Search	Base	SC-7	Supports	PT-3 (partially supports)
Disable Search Location	Base	PT-3	Supports	SC-42 (partially supports)

Setting	Profile	Control	Relationship	Also Supports
Disable Cortana *	Base	CM-7	Supports	-
Disable Cross-Device Experiences	Layer	AC-20	Supports	CM-7 (partially supports)
Disable Settings Sync	Base	AC-20	Supports	PT-3 (incidental)
Disable Settings Sync User Override	Base	CM-6	Supports	-
Disable Cloud Clipboard	Base	AC-20	Supports	SI-12 (supports)
Disable Find My Device	Base	PT-3	Supports	SC-42 (supports)

4.3 App Permissions

Setting	Profile	Control	Relationship	Also Supports
Disable Location Services	Layer	PT-3	Supports	SC-42 (partially supports)
Deny App Access to Location	Layer	PT-3	Supports	SC-42 (partially supports)
Deny App Access to Camera	Layer	PT-3	Supports	SC-15 (partially supports)
Deny App Access to Microphone	Layer	PT-3	Supports	SC-15 (partially supports)
Deny App Access to Radios	Base	CM-7	Supports	-
Deny App Access to Motion	Base	PT-3	Supports	SC-42 (partially supports)
Deny Sync with Unpaired Devices	Base	AC-20	Supports	-
Deny App Access to Trusted Devices	Layer	AC-20	Supports	-
Deny App Access to Account Info	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Contacts	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Calendar	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Email	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Messaging	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Phone Calls	Layer	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Call History	Layer	PT-3	Supports	AC-3 (partially supports)
Deny Background App Execution	Layer	CM-7	Supports	-
Deny App Access to Notifications	Base	PT-3	Supports	SI-12 (incidental)
Deny Voice Activation	Base	PT-3	Supports	SC-15 (partially supports)
Deny Voice Activation Above Lock	Base	AC-11	Supports	SC-15 (supports)
Deny App Access to Tasks	Base	PT-3	Supports	AC-3 (partially supports)
Deny App Access to Diagnostics	Base	AC-3	Supports	CM-7 (partially supports)

4.4 Windows Features

Setting	Profile	Control	Relationship	Also Supports
Disable All Store Apps	Layer	CM-7	Supports	CM-10 (supports)
Disable Auto Download and Install of Updates	Layer	CM-3	Supports	-
Suppress Store App Recommendations (Policy)	Base	CM-7	Supports	-
Suppress Store App Recommendations (Source)	Base	CM-7	Supports	-
Disable SmartScreen for Store Apps	Base	SC-7	Partially supports	-
Disable All Spotlight Features	Base	CM-7	Supports	PT-3 (incidental)
Disable Cloud Optimized Content	Base	CM-7	Supports	-
Disable Widgets	Base	CM-7	Supports	-
Disable News and Interests *	Base	CM-7	Supports	-
Disable Recommendations	Base	CM-7	Supports	PT-3 (incidental)
Disable App Launch Tracking	Base	SI-12	Supports	PT-3 (supports)
Disable Online Speech Recognition	Base	PT-3	Supports	SC-7 (partially supports)
Disable Speech Model Updates	Base	SC-7	Partially supports	-
Disable Notification Network Traffic	Layer	SC-7	Supports	-
Disable Online Tips	Base	CM-7	Supports	SC-7 (partially supports)
Disable App URI Handlers	Base	CM-7	Supports	-
Disable Auto Download Map Data	Base	CM-7	Supports	SC-7 (partially supports)
Disable Unsolicited Map Network Traffic	Base	SC-7	Supports	-
Disable Activity Feed *	Base	SI-12	Supports	PT-3 (supports)
Disable Publish User Activities *	Base	PT-3	Supports	-
Disable Upload User Activities *	Base	PT-3	Supports	AC-20 (partially supports)

4.5 Windows Update

Setting	Profile	Control	Relationship	Also Supports
Disable Insider Preview Builds	Base	CM-3	Supports	SI-7 (partially supports)
Disable Peer-to-Peer Update Sharing	Base	SC-7	Supports	CM-7 (partially supports)
Disable Disk Health Model Updates	Base	CM-7	Partially supports	-
Disable Services Configuration	Base	CM-3	Supports	CM-6 (supports)

4.6 Internet Explorer

Setting	Profile	Control	Relationship	Also Supports
Disable Suggested Sites *	Base	PT-3	Supports	SC-7 (partially supports)
Disable Enhanced Suggestions *	Base	PT-3	Supports	-
Disable Browser Geolocation *	Base	PT-3	Supports	SC-42 (partially supports)
Disable AutoComplete for Web Addresses *	Base	SI-12	Supports	-
Disable Feed Background Sync *	Base	SC-7	Supports	CM-7 (partially supports)
Disable IE SmartScreen *	Base	SC-7	Partially supports	-
Disable ActiveX VersionList Download *	Base	SC-18	Supports	SI-7 (partially supports)
Set IE Home Page to Blank *	Base	CM-6	Supports	-
Lock IE Home Page Setting *	Base	CM-6	Supports	-
Disable IE First Run Wizard *	Base	CM-7	Partially supports	-
Set IE New Tab to Blank *	Base	CM-7	Partially supports	-
Disable Compatibility View Editing *	Base	CM-6	Supports	-
Disable Flip Ahead *	Base	PT-3	Supports	SC-7 (partially supports)

4.7 Background Services

Setting	Profile	Control	Relationship	Also Supports
Disable Device Metadata Retrieval	Base	SC-7	Supports	PT-3 (partially supports)
Disable Font Streaming	Base	SC-7	Supports	CM-7 (partially supports)
Disable KMS Online Validation *	Base	SC-7	Supports	-
Disable Teredo	Base	SC-7	Supports	-
Disable License Manager Service	Layer	CM-7	Supports	-

4.8 Telemetry and Reporting

Setting	Profile	Control	Relationship	Also Supports
Exclude Device Name from Diagnostic Data	Base	SI-19	Supports	PT-3 (supports)
Limit Diagnostic Log Collection	Base	SI-12	Supports	PT-3 (partially supports)
Limit Dump Collection	Base	SC-28	Supports	SI-12 (partially supports)
Disable Windows Error Reporting	Base	PT-3	Supports	-
Disable Application Telemetry	Base	PT-3	Supports	CM-7 (partially supports)
Disable Inventory Collector	Base	PT-3	Supports	-
Disable Inking and Typing Data Collection	Base	PT-3	Supports	-

4.9 Security Defaults

Setting	Profile	Control	Relationship	Also Supports
Disallow AutoPlay for Non-Volume Devices	Base	MP-7	Supports	SI-3 (partially supports)
Disable AutoRun Command Execution	Base	MP-7	Supports	SI-3 (partially supports)
Disable AutoPlay	Base	MP-7	Supports	SI-3 (partially supports)
Disable Multicast Name Resolution	Base	CM-7	Supports	IA-5 (partially supports)
Disable Smart Multi-Homed Name Resolution	Base	SC-7	Supports	-
Disable Lock Screen App Notifications	Base	AC-11(1)	Partially supports	-
Disable Automatic Sign-In After Restart	Base	IA-11	Supports	AC-11 (partially supports)
Disable Local Account Security Questions	Base	IA-5	Supports	-
Disable Fast Startup	Base	SC-28	Partially supports	-
Disable Indexing of Encrypted Files	Base	SC-28	Supports	-
Disable MDM Enrollment	Base	CM-7	Supports	AC-3 (partially supports)

4.10 Activity and History

Setting	Profile	Control	Relationship	Also Supports
Disable Recently Opened Document History	Base	SI-12	Supports	PT-3 (partially supports)
Remove Recently Added List from Start Menu	Base	SI-12	Supports	PT-3 (partially supports)
Disable File Explorer Search History	Base	SI-12	Supports	-
Disable Search History	Base	SI-12	Supports	-
Disable File Explorer Account Insights	Base	CM-7	Supports	AC-20 (partially supports)
Disable Clipboard History	Base	SI-12	Supports	PT-3 (partially supports)

4.11 Content Delivery

Setting	Profile	Control	Relationship	Also Supports
Disable Windows Tips	Base	CM-7	Supports	-
Disable Consumer Account State Content	Base	CM-7	Supports	PT-3 (incidental)
Disable Spotlight Collection on Desktop	Base	CM-7	Supports	-
Disable Windows Welcome Experience	Base	CM-7	Supports	-
Disable Spotlight on Action Center	Base	CM-7	Supports	-
Disable Spotlight on Settings	Base	CM-7	Supports	-
Disable Search Highlights	Base	CM-7	Supports	-
Disable Cloud Search	Base	SC-7	Supports	PT-3 (partially supports)
Disable Push To Install Service	Base	CM-11	Supports	CM-7 (partially supports)
Disable Account Notifications in Start	Base	CM-7	Supports	-

4.12 Windows Applications

Setting	Profile	Control	Relationship	Also Supports
Disable Windows Copilot *	Base	CM-7	Supports	-
Disable Recall *	Base	SI-12	Supports	PT-3 (supports)
Disable Click to Do	Base	CM-7	Supports	PT-3 (partially supports)
Disable Settings Agentic Search	Base	CM-7	Supports	PT-3 (partially supports)
Disable Phone-PC Linking	Layer	AC-20	Supports	CM-7 (partially supports)
Disable Game Recording and Broadcasting	Base	CM-7	Supports	SI-12 (partially supports)
Disable Windows Media DRM Internet Access	Base	SC-7	Supports	-
Disable CD and DVD Media Information Retrieval	Base	SC-7	Supports	PT-3 (partially supports)
Disable Music File Media Information Retrieval	Base	SC-7	Supports	PT-3 (partially supports)

5. Control Narratives

Narratives are provided for the controls carrying the most weight in this baseline and for those where the character of the contribution is not evident from the mapping table. Where a control has lettered elements, the narrative reports which element the baseline reaches, because that is the granularity SP 800-53A assessment objectives use.

5.1 PT-3, Personally Identifiable Information Processing Purposes

38 settings and 60 citations, the largest grouping in the baseline. Origination: O.

PT-3 has four elements. The baseline reaches exactly one of them.

Element	Requirement	Baseline
PT-3a	Identify and document the purposes for processing PII	Organizational
PT-3b	Describe the purposes in public privacy notices and policies	Organizational
PT-3c	Restrict processing of PII to what is compatible with the identified purposes	All 38 settings support this element
PT-3d	Monitor changes in processing and implement mechanisms accordingly	Organizational

Every PT-3 contribution in this baseline lands on element (c), which is purpose limitation in the privacy sense: processing is confined to what the identified purpose supports. That is a more useful statement than any count, and it is the shape of most contributions here: the device can restrict processing, and it cannot identify purposes, publish notices, or monitor change.

The settings fall into three groups by mechanism. **Collection channels with policies of their own**: Windows Error Reporting, Application Impact Telemetry, and the inventory collector each have a policy separate from the `AllowTelemetry` level, and disabling one closes that channel whatever the level permits. That is the most consequential contribution in the file, because it addresses exposure a system owner would reasonably believe was already closed. **Data minimization within retained collection**: excluding the device name, limiting diagnostic log collection, and limiting dump collection reduce what is retained and transmitted where collection cannot be disabled. **On-device records accumulating without user action**: document and application history, search history, and clipboard history, addressed under SI-12 where retention is the objective.

`Exclude Device Name from Diagnostic Data` is assigned to SI-19, De-identification, rather than to PT-3 as its first control. SI-19a requires removing identifying elements from datasets, which is precisely what the setting does to a telemetry payload. SI-19b, evaluating the effectiveness of de-identification, is organizational and untouched.

5.2 CM-7, Least Functionality

38 settings. Origination: O/S.

The baseline disables features that ship enabled and that a standalone device does not require: content delivery surfaces, cloud search, AI features, device linking, game capture, media information retrieval, and MDM enrollment.

The character of this coverage needs stating precisely, and CM-7's origination states it for us. CM-7 is designated `O/S`, and the organizational half is the determination of what counts as essential. That determination is not one a baseline can make on a system owner's behalf. This baseline encodes a specific judgment: that a standalone personal or business device does not require Microsoft consumer content delivery, AI assistants, or cross-device linking. For an organization whose users depend on Phone Link or Copilot, the corresponding settings are a functionality reduction rather than a control improvement.

The layered profile design accommodates this. The No Store Apps layer is separated from the base precisely because dependence on the Microsoft account and Store varies by device.

Where CM-7b prohibits "organization-defined functions, ports, protocols, and software," the baseline's least-functionality settings are a concrete value supplied for that organization-defined parameter. That is the accurate description of the contribution: the baseline proposes a value, and the organization adopts or amends it.

5.3 SC-7, Boundary Protection

19 settings. Origination: S.

SC-7 is one of the few high-count controls here that NIST designates system-implemented, so device configuration can form part of the implementation rather than only supporting it.

Most of these settings close outbound connections initiated by individual components: cloud search, web results in Search, Windows Media DRM license acquisition, media metadata retrieval, device metadata, font streaming, map data, and push notification traffic. They reduce the set of unsolicited outbound destinations. They are not a substitute for host or network firewall policy, which the baseline does not configure.

Two deserve separate mention. `Disable Teredo` is the cleanest assignment in the file: Teredo tunnels IPv6 through an IPv4 NAT, which is a boundary traversal a host firewall rule set does not necessarily observe. `Disable Smart Multi-Homed Name Resolution` stops Windows sending DNS queries across all active interfaces simultaneously, which can leak queries across a VPN tunnel onto the local interface.

`Disable Multicast Name Resolution` is assigned to CM-7 rather than to SC-20 or SC-21. Those controls concern a system providing secure name resolution through DNSSEC, and disabling LLMNR configures no such service. The honest assignment is the disabling of a nonessential

protocol, with a partial contribution to IA-5 because LLMNR poisoning is a path to capturing authenticator material.

5.4 SI-12, Information Management and Retention

10 settings. Origination: O.

SI-12 requires managing and retaining information in accordance with applicable requirements. The baseline reduces what the device retains without user action: recently opened document history, the recently added list, File Explorer and Search history, clipboard history, app launch tracking, the activity feed, and Recall's screenshot store.

The control is organization-implemented, and the gap is worth naming. SI-12 asks an organization to determine retention requirements and manage information against them. The baseline supplies no retention determination. It removes accumulation the user did not ask for and could not easily inspect, which supports the objective without meeting it.

`Disable Clipboard History` is the setting here a system owner most needs to know about. A clipboard retains whatever was copied into it, which routinely includes credentials pasted from a password manager, and also personal, payment, and employee data. The retention is invisible and the exposure is broad.

5.5 AC-20, Use of External Systems

8 settings. Origination: O.

These settings close paths by which device data reaches a system the organization does not control: OneDrive file storage, settings synchronization, cloud clipboard, cross-device experiences, Phone Link, sync with unpaired devices, and app access to trusted devices, together with the Microsoft account sign-in service that underpins several of them.

AC-20 requires an organization to establish terms for the use of external systems. The baseline establishes no terms. It removes the mechanisms, which is a stronger action in one direction and no action at all in the other: a device with these settings applied has fewer external system paths, and the organization still has no policy governing the ones a user might introduce.

5.6 MP-7, Media Use

3 settings. Origination: O.

Three settings act together, and the interdependency is load-bearing. `Disable AutoPlay` suppresses the AutoPlay dialog for drive-type devices. `Disallow AutoPlay for Non-Volume Devices` extends coverage to cameras, phones, and other MTP devices not presented as drives. `Disable AutoRun Command Execution` prevents `AutoRun.inf` command execution independently of whether AutoPlay is active.

Any subset leaves a gap. Applying only the first two still permits `AutoRun.inf` execution. Applying only the third still presents the AutoPlay dialog for non-volume devices. An assessor evaluating this control against the baseline should confirm all three rather than sampling one.

The relationship is `Supports` and not more. MP-7 is organization-implemented and requires restricting or prohibiting the use of removable media, which is a policy determination. These settings address automatic execution from media once connected. The baseline does not address media connection itself, which needs a separate mechanism.

5.7 SC-15 and SC-42, Collaborative Computing and Sensor Data

No first-control assignments, 10 partial contributions. Origination: S for both.

Eight settings deny application access to a sensor: location twice, camera, microphone, motion, search location, browser geolocation, and voice activation.

Both controls are aimed at covert activation. SC-15a prohibits remote activation of collaborative computing devices, which its discussion defines to include cameras and microphones. SC-42a prohibits the use of sensor-bearing devices in defined areas or the remote activation of sensing capabilities. An application holding microphone permission and passively monitoring for a keyword is that threat whatever the activation path, and voice activation is the clearest instance, since always-on microphone consumption is not a risk of the feature but its documented behavior. Denying the capability removes the precondition.

Coverage is partial for two reasons, both documented rather than inferred:

1. **UWP scope.** Each of these settings carries the advisory `Applies to UWP apps only. Win32 desktop apps are not affected.` On a typical Windows device Win32 software is the larger share of what is installed, so the baseline closes one activation path and leaves the wider one open. `Disable Location Services` is the exception, disabling the system-wide location platform rather than a UWP capability.

2. **Element (b) untouched.** Both controls require an explicit indication of sensor use. The baseline configures nothing toward it. Windows provides its own camera and microphone indicators, and the baseline neither establishes nor verifies them.

The first control for these settings is PT-3, because the objective they serve is limiting the processing of personally identifiable information, and sensed location, imagery, audio, and motion are all PII.

5.8 AC-11, IA-5, and IA-11, Device Lock and Authentication

3 settings. Origination: S, O/S, O/S.

`Disable Automatic Sign-In After Restart` supports IA-11, Re-authentication, by preventing Windows from signing the user back in and restoring session state following an update-initiated restart without authentication having occurred.

`Disable Local Account Security Questions` supports IA-5, Authenticator Management, by removing the security-question recovery mechanism for local accounts. Security questions are a weak authenticator: answers are frequently discoverable, are not revocable, and are reused across services. Removing the mechanism eliminates an alternate authentication path weaker than the primary one.

`Disable Lock Screen App Notifications` is assigned to AC-11(1) as a partial contribution, and the limit should be stated. AC-11(1), Pattern-Hiding Displays, requires concealing information *previously visible* on the display. Notifications rendered after the device locks are new information, not previously visible information, so the control text does not directly cover the behavior. The objective is nonetheless served: an email notification exposes sender, subject, and time to an unauthenticated observer, which in a sensitive environment is disclosure on its own. No Rev. 5 control addresses post-lock notification rendering directly, and AC-11(1) is the nearest.

`Deny Voice Activation Above Lock` supports AC-11 directly, preventing microphone interaction with a locked device.

The baseline does not configure password policy, account lockout thresholds, screen lock timeout, or multifactor authentication. Coverage in these families is limited to removing specific weak defaults.

5.9 SC-28, Protection of Information at Rest

3 settings. Origination: S.

`Limit Dump Collection` reduces memory content written to disk. `Disable Indexing of Encrypted Files` prevents the search index caching decrypted content of encrypted files. `Disable Fast Startup` closes one of two paths by which a kernel session image is written to disk on shutdown.

Two limits. First, SC-28 in its broader sense concerns cryptographic protection of stored information, and the baseline configures no encryption mechanism. Its contribution is limited to reducing what is written in the clear. Second, the baseline deliberately declines `Disable Hibernation`, so the hibernation write path remains open, for the reasoning given in Section 8. A system owner who applies this baseline and considers the data-at-rest objective addressed for memory images will be incorrect.

5.10 CM-3 and CM-6, Change Control and Configuration Settings

3 and 4 settings. Origination: O and O/S.

`Disable Services Configuration` is the strongest CM-3 assignment in the file. It prevents Microsoft pushing remote configuration changes to Windows components, which is configuration change control in its most literal form: a change to the device's configuration that would otherwise occur without review or approval. `Disable Insider Preview Builds` keeps the device off a pre-release channel.

Under CM-6, `Disable Settings Sync User Override` and the three Internet Explorer home page and Compatibility View settings prevent a user overriding an applied configuration, which supports the enforcement element of the control. Three of those four are subject to a scoping consideration, discussed in Section 6.2.

The larger CM-6 contribution is at the artifact level rather than the setting level, and is recorded in Section 3.4.

6. Coverage Analysis

6.1 Control Origination

NIST designates every control as organization-implemented (`O`), system-implemented (`S`), or both (`O/S`), carried in the OSCAL catalog as an implementation level. This is the framework's own position on the responsibility split, and it is the most important structural fact about this baseline.

Control	Title	First	All	Origination
PT-3	Personally Identifiable Information Processing Purposes	38	60	O
CM-7	Least Functionality	38	48	O/S
SC-7	Boundary Protection	19	24	S
SI-12	Information Management and Retention	10	14	O
AC-20	Use of External Systems	8	10	O
CM-6	Configuration Settings	4	6	O/S
CM-3	Configuration Change Control	3	3	O
MP-7	Media Use	3	3	O
SC-28	Protection of Information at Rest	3	3	S
AC-3	Access Enforcement	1	10	S
AC-11	Device Lock	1	2	S
IA-5	Authenticator Management	1	2	O/S
AC-11(1)	Device Lock, Pattern-Hiding Displays	1	1	S
CM-11	User-Installed Software	1	1	O
IA-11	Re-authentication	1	1	O/S
SC-18	Mobile Code	1	1	O
SI-19	De-identification	1	1	O/S
SC-42	Sensor Capability and Data	0	6	S
SC-15	Collaborative Computing Devices and Applications	0	4	S
SI-3	Malicious Code Protection	0	3	O/S
SI-7	Software, Firmware, and Information Integrity	0	2	O/S
CM-10	Software Usage Restrictions	0	1	O
Total		134	206	

`First` counts settings whose primary assignment is the row. `All` includes partial and incidental contributions.

Only 25 of the 134 assignments are against controls a system implements on its own. Of the rest, 64 fall on controls NIST marks `O` and 45 on controls marked `O/S`. PT-3 and SI-12 are the two largest organization-implemented groupings and carry 48 between them.

This is the honest headline of the coverage analysis, and it is more useful than a coverage percentage, because it tells a system owner how much of what this baseline contributes must be paired with organizational process before any control is satisfied.

`MP-7` deserves the same caution. It is organization-implemented, so the three interdependent AutoPlay settings support it and do not address it.

6.2 Scoping Considerations

21 of the 112 base settings do not take effect on a standard, retail-licensed Windows 11 25H2 device.

The SP 800-53 glossary defines **scoping considerations** as part of tailoring guidance providing specific considerations on the applicability of controls, enumerating policy or regulatory, technology, physical infrastructure, system component allocation, public access, scalability, common control, operational, and security objective. Every case below is a technology, operational, or licensing consideration applied at the setting level. Naming the consideration is more useful than calling the setting inert, because the assessor's own scoping decision depends on which condition applies to the device in front of them.

Condition	Count	Settings
Feature removed after Windows 10	4	News and Interests, Activity Feed, Publish User Activities, Upload User Activities
Feature removed in Windows 11 23H2	1	Disable Cortana
Policy deprecated in Windows 11 24H2	1	Disable Windows Copilot
Requires Copilot+ hardware	1	Disable Recall
Volume-licensed devices only	1	Disable KMS Online Validation
Internet Explorer application chrome, no surface on Windows 11	8	Suggested Sites, Enhanced Suggestions, Set IE Home Page to Blank, Lock IE Home Page Setting, IE First Run Wizard, Set IE New Tab to Blank, Flip Ahead, Feed Background Sync
Internet Explorer platform layer, effective only for content rendered in IE mode	4	ActiveX VersionList Download, IE SmartScreen, Browser Geolocation, Compatibility View Editing
Registry scope shared with File Explorer, effect on Windows 11 unverified	1	Disable AutoComplete for Web Addresses

Only the first three are version conditions. Two are hardware and licensing conditions applying equally on Windows 10.

These settings are carried deliberately. One profile serves the whole supported range rather than splitting into a variant per build, and a setting that does not take effect costs nothing to apply. The consequence for coverage is specific: **coverage should be read against the settings effective on the configuration being assessed, not against the count applied.**

The Internet Explorer settings are not uniformly inert. The Internet Explorer 11 desktop application is retired and not present on Windows 11. The IE platform, MSHTML, remains, and Microsoft Edge's IE mode renders content with it. Eight of the thirteen settings target the IE application chrome and have no surface on Windows 11 regardless of configuration. Four target the platform layer and act on rendered content, so they are effective where IE mode is configured, which requires an administrator to enable it with a site list and which a standalone device does not have by default. Whether each policy is honored in IE mode is not documented by Microsoft at the per-policy level and has not been tested here.

`Disable AutoComplete for Web Addresses` is a separate case. The definitions file maps it to the Internet Explorer policy `Turn off the auto-complete feature for web addresses`, but its registry target is the shared File Explorer AutoComplete key rather than an Internet Explorer key. Whether it suppresses shell autocomplete on Windows 11 is unverified and is not asserted here in either direction.

Coverage by control, where `Conditional` counts assignments subject to one of these considerations:

Control	Applied	Conditional	Unconditional on target
PT-3	38	6	32
CM-7	38	5	33
SC-7	19	3	16
SI-12	10	3	7
CM-6	4	3	1
SC-18	1	1	0

CM-6 is the sharpest case: three of its four setting-level assignments are Internet Explorer chrome settings, so on Windows 11 the baseline's setting-level CM-6 contribution reduces to one, `Disable Settings Sync User Override`. Its artifact-level contribution, in Section 3.4, is unaffected.

SC-18, Mobile Code, has a single assignment, `Disable ActiveX VersionList Download`, and it is in the IE platform-layer group. The baseline's only mobile-code contribution is to ActiveX, and ActiveX executes on Windows 11 only within IE mode. An assessor crediting SC-18 on the strength of this baseline should confirm whether IE mode is configured, and treat the contribution as absent if it is not.

6.3 Controls Not Addressed

The baseline does not address, and should not be credited toward: AU-2 through AU-11 (audit event selection, content, storage, protection, and retention), AC-2 (account management), AC-6 (least privilege), IA-2 (identification and authentication of users), SC-13 (cryptographic protection), SI-4 (system monitoring), SI-7 (software and information integrity, beyond two partial contributions), CM-8 (system component inventory), and the CP, IR, RA, PL, PM, AT, and SA families in full. SI-2(7), Root Cause Analysis, added in Release 5.2.0, is wholly organizational and unaddressed.

Several of these are unaddressable by device configuration on a standalone system with no centralized infrastructure. This is worth checking against NIST's own privacy control baseline, which contains 96 controls: this baseline's 134 settings touch three of them, PT-3, SI-12, and SI-19. The remainder are policy, program management, training, incident response, assessment, and planning controls. **NIST's privacy baseline is a program, not a configuration**, and a device baseline can only ever touch the part of it that a device implements.

7. Where the Baseline Works Against a Control Objective

Nine settings carry a cost alongside their benefit. For six of them the cost falls on another control objective. For the other three, `Disable Find My Device`, `Disable Windows Error Reporting`, and `Disable Disk Health Model Updates`, it falls on a capability no control covers.

Four cases below treat the substantial ones. The smallest costs, `Disable Enhanced Notifications`, `Disable Windows Error Reporting`, and `Disable Disk Health Model Updates`, are noted at the end of the section rather than given a case of their own.

All are deliberate, and all should reach a system owner before the baseline is applied rather than being discovered during assessment.

7.1 Defender Cloud Protection

`Disable MAPS Reporting` and `Disable Sample Submission` support PT-3 by closing a channel that reports file hashes, and in the case of sample submission the files themselves, to Microsoft. Both also reduce Defender's cloud-assisted detection, which is the component that responds fastest to threats no signature covers yet, so both work against SI-3.

The base accepts that reduction because the remaining malicious code protection posture is not thin. Signatures, the local detection engine, behavior monitoring, and system-wide SmartScreen all continue to operate, and the base retains system-wide SmartScreen for this reason.

Verdict: the base trades bounded, redundant detection capability for a continuous reporting channel, and records the trade here. A system owner whose malware exposure justifies cloud-assisted detection should exclude both settings before applying the profile.

7.2 SmartScreen for Store Apps and Internet Explorer

`Disable SmartScreen for Store Apps` closes a narrow URL reporting channel and removes a narrow SI-3 check on web content loaded by Store apps. `Disable IE SmartScreen` does the same within Internet Explorer.

Verdict: the base keeps the broad filter and drops the narrow ones. System-wide SmartScreen stays, providing malware and phishing protection for files and applications. Store apps are vetted and carry little risk in the content they load, and Internet Explorer is not present on Windows 11. This is a decision about which filters to keep and is not a compensating control in the SP 800-53B sense: nothing is substituting for a control that could not be implemented.

7.3 Find My Device

`Disable Find My Device` supports PT-3 and contributes to SC-42 by closing a continuous, high-sensitivity location stream. The cost is device recovery capability after theft.

Verdict: the privacy cost is continuous and the recovery benefit is conditional, requiring both location services and a Microsoft account, and mattering mainly on portable devices. The nearest control on the cost side is PE-20, Asset Monitoring and Tracking, which employs asset location technologies to track assets within organization-defined controlled areas. The mapping does not assign it. Find My Device recovers a device that has left, where PE-20 concerns assets remaining in authorized locations, and the fit is too loose to credit. It is worth naming because PE-20's own

discussion directs organizations to consult privacy counsel before deploying asset location technologies, which is the same tension this setting resolves in the other direction.

7.4 Store Application Updates

`Disable Auto Download and Install of Updates` supports CM-3 by moving Store application updates from automatic to administrator-initiated, and works against SI-2 for those applications.

Verdict: the cost is nil in context. This setting is in the No Store Apps layer, and the same layer disables Store applications entirely. An application that cannot launch does not need patching. This is worth stating because it demonstrates that a layer is internally coherent rather than a collection of related settings, and because the same setting applied without the rest of the layer would carry a real SI-2 cost.

`Disable Enhanced Notifications` reduces Defender alerting to the user, a small SI-4 reduction. `Disable Windows Error Reporting` forgoes Microsoft's analysis of crash reports, and `Disable Disk Health Model Updates` removes a failure-prediction data feed, capability costs rather than security ones. Crash dumps written to disk before Windows Error Reporting is disabled are not removed, and a system owner applying it for privacy reasons should clear existing dumps separately.

8. Settings the Baseline Declines

The definitions files catalog 162 settings. The curated profiles carry 134. The 28 the baseline declines are as much a part of its design as the 134 it applies, and each is declined to protect a control objective or because it falls outside this target's scope.

These decisions are the configuration-level analogue of **tailoring**, which SP 800-53 defines as modifying a control baseline by applying scoping considerations, selecting compensating controls, assigning values to control parameters, and supplementing the baseline. The analogy should not be overdrawn: tailoring in SP 800-53B operates on a set of controls, and these decisions operate on a set of settings. The reasoning is parallel and the object is not the same. A reader arriving from ISO/IEC 27001 will recognize the shape of the table below, which serves the purpose a Statement of Applicability serves there: recording which controls apply, which do not, and the justification for each exclusion.

Declined setting or group	Count	Objective protected	Control
Windows Update settings	8	The device continues to receive and install security patches without administrative action	SI-2
Microsoft Edge and Edge Update	14	Not a protection. Scope boundary, deferred to the Edge target	None
Set Time Sync to NoSync, Disable NTP Client	2	Clock accuracy, on which certificate validity windows, time-based authenticators, and audit timestamps all depend	SC-45, AU-8, IA-5
Disable Automatic Root Certificate Updates	1	Certificate path validation continues to work as trust anchors change	SC-17
Disable SmartScreen (system-wide)	1	Broad malware and phishing protection for files and applications	SI-3
Disable NCSI Active Tests	1	Connectivity detection that applications and services depend on	Availability
Disable Hibernation	1	Hibernation remains available. The data-at-rest gain applies only to an unencrypted disk	Functionality

8.1 Windows Update

The eight declined update settings are the most consequential decision in the baseline, and reading SI-2 at element level shows the trade is finer than it first appears.

SI-2 has four elements, and two of them pull against each other. **SI-2b** requires testing updates for effectiveness and potential side effects *before installation*. **SI-2c** requires installing security-relevant updates *within an organization-defined time period* of release. Automatic installation serves (c) and precludes (b). Disabling it serves (b) and transfers (c) to an operator who may or may not perform it. **The setting therefore trades within SI-2, not between SI-2 and CM-3.**

The base declines it because on an unattended standalone device an unperformed (c) fails silently and accumulates known vulnerabilities, while an unperformed (b) costs a test a single-device owner was unlikely to run. That verdict would reverse on a device with a maintenance schedule and an operator.

Four of the eight would additionally blank or redirect the update source. The Release 5.2.0 discussion for SI-2 states that organizations verify software and firmware updates come from authorized sources prior to downloading. Declining those four keeps the device pointed at its authorized source.

Verdict: security patching is not traded away on a device that may have no operator. SI-2's own discussion contemplates a controlled patching environment for mission-critical systems, and a standalone personal or business device is generally not in that class.

8.2 Time Synchronization and Trust Anchors

`Set Time Sync to NoSync` and `Disable NTP Client` would stop the device synchronizing its clock. `Disable Automatic Root Certificate Updates` would stop it acquiring new trust anchors.

Clock drift breaks TLS certificate validation, because validity windows are evaluated against local time, and breaks time-based one-time password authenticators. It also compromises AU-8, Time Stamps, which requires system clocks to be used to generate reliable timestamps for audit records. A device with a drifting clock cannot produce trustworthy audit records even where audit records are being kept.

Verdict: time, certificate, and update integrity are never traded for privacy. These are the clearest cases in the baseline of a privacy gain that is not worth its security cost, and they are declined without qualification.

9. Notes for Assessors

What the evidence demonstrates, and what it does not. Snapshot Mode captures current system state as a profile, which can be compared against the applied baseline profile to confirm settings are in effect. This is **point-in-time evidence of design and implementation**: it establishes that a setting was configured when the snapshot ran. On its own it does not establish **operating effectiveness**, meaning that the setting held throughout a period under assessment.

The enforcement mechanism changes that answer, and it differs by edition. On Pro, Enterprise, Education, and LTSC, the 123 policy-managed settings listed in Section 3.3 are re-applied by the Group Policy engine at every refresh. A manual change is reverted at the next cycle without administrative action. For those settings the assessment question is not whether they drifted but whether the policy remained in place, which is examinable directly in Local Group Policy and is closer to a continuously operating control than a point-in-time reading suggests.

For the 11 settings outside the policy branches, and for every setting on Home edition, no mechanism re-asserts the value. A local administrator can change it and nothing restores it, so detecting drift depends on re-running Snapshot Mode and comparing output, which is a manual activity. An assessment requiring evidence of operating effectiveness across a period should treat

those settings differently from the 123, and should collect the policy artifact rather than the registry value where one exists.

Collect evidence at the layer that is authoritative. On non-Home editions the Local Group Policy entry is the authoritative record for the 123 managed settings, because it is what the refresh re-applies, and a registry read alone cannot distinguish a managed value from one an administrator set manually. On Home the registry is the only record there is.

Assessment methods. In SP 800-53A terms, the assessment objects in this baseline are **mechanisms**, and the applicable methods are **EXAMINE** for the configuration or policy state and **TEST** for the snapshot comparison. Nothing in this baseline is established by **INTERVIEW**.

Two settings are registry-only on all editions. `Disable Fast Startup` and `Disable Hibernation` have no Group Policy equivalent, so an assessor verifying through Group Policy alone will not observe them. `Disable Hibernation` is declined by the base in any case.

One Group Policy name is inverted. The policy governing File Explorer account insights is named `Show files based on your account and cloud provider activity`. It must be set to **Enabled** to prevent the files from being shown, writing `DisableGraphRecentItems` to `1`. Setting it to Disabled enables the feature. An assessor reading policy state rather than registry values should note the inversion.

The baseline is not machine-readable security content. Its settings carry no Common Configuration Enumeration identifiers and its profiles are not SCAP content, so an automated assessment tool consuming XCCDF or OVAL cannot evaluate this baseline directly. Verification is through the toolkit's own snapshot comparison or through manual examination of the registry or policy state.

Scoping. Before crediting any control, confirm which of the conditions in Section 6.2 apply to the device being assessed. The baseline is designed to serve Windows 10 and Windows 11 from a single profile, which means a Windows 11 device carries settings that take no effect on it.

10. Traceability

Every setting in this mapping traces to four places:

1. Its entry in a curated profile, Policy-Windows-Base.psd1 or Policy-Windows-NoStoreApps.psd1, giving the registry path, value name, type, and value applied.

2. Its definition in Policy-MicrosoftPrivacyConnections.psd1 or Policy-WindowsPrivacyDefaults.psd1, giving the Group Policy path where one exists and any advisory on side effects or applicability.
3. Its research and editorial rationale in the corresponding definitions reference document, under definitions/reference/.
4. The curation decision that placed it in the base or the layer, in profiles/reference/Policy-Windows.md.

Control text, assessment objectives, and implementation designations are drawn from NIST's OSCAL catalog for SP 800-53 Revision 5, Release 5.2.0, published at `usnistgov/oscal-content`.

Settings in `Policy-WindowsPrivacyDefaults` were identified and verified through direct system analysis rather than transcribed from a published checklist. Settings in `Policy-MicrosoftPrivacyConnections` are drawn from Microsoft's guidance on managing connections from Windows to Microsoft services, with documented deviations where that guidance is internally inconsistent.

11. References

NIST SP 800-53 Revision 5, Release 5.2.0. *Security and Privacy Controls for Information Systems and Organizations.* Control text, control discussion, and implementation designations. Taken from NIST's OSCAL catalog at usnistgov/oscal-content, which tracks the current release. The published PDF of Revision 5 predates Releases 5.1.1 and 5.2.0.

NIST SP 800-53A Revision 5. *Assessing Security and Privacy Controls in Information Systems and Organizations.* Assessment objectives, assessment methods, and assessment objects, carried in the same OSCAL catalog.

NIST SP 800-53B. *Control Baselines for Information Systems and Organizations.* Control baselines and tailoring guidance, cited for the definitions of tailoring and compensating controls.

NIST IR 8278 Revision 1 and NIST IR 8278A Revision 1. *National Online Informative References (OLIR) Program.* The relationship types used to classify a mapping, and the supportive relationship mapping this document performs.

Microsoft. *Manage connections from Windows operating system components to Microsoft services.* The source for the settings in `Policy-MicrosoftPrivacyConnections`, with deviations recorded in that file's reference document.

Microsoft. *Internet Explorer (IE) mode troubleshooting and FAQ.* Cited in Section 6.2 for the dependency of IE mode on the Internet Explorer platform.

12. Revision History

Version	Date	Change
1.0	2026-09-09	Initial issue
1.1	2026-09-10	Corrected control counts and characterizations. Conclusions unchanged
1.2	2026-09-10	Clarified section 7 membership. Counts and conclusions unchanged
1.3	2026-09-23	Withdrew the SI-4 cost of disabling Windows Error Reporting, clarified the relationship of three collection channels to the diagnostic data level, added AC-3 to Deny App Access to Tasks, corrected three characterizations, and aligned table columns. Conclusions unchanged