Security impact analysis

HARBORLIGHT Predictive Maintenance and Readiness Assistant

Assistant drafts work orders; FailurePredictor 3.4.1; prompt template 14

System	HARBORLIGHT Predictive Maintenance and Readiness Assistant (HARBORLIGHT), SYS-0001
Program	CALC Readiness Modernization
System owner	Priya Raman
Environment	Production, Controlled
Change	CHG-0006, version 6 to 7, recorded from a model edit
Analyzed	2026-11-11 02:22 UTC by Kendrake Delta 1.0.0 with rule pack kendrake-dependency@2.0.0
Analysis hash	`b889a341cdf31410d6e7e92bbba8e284ed7a313b26a4d20b2bfb0d7c832fc0c1`
Record generated	2026-11-11 02:22 UTC by Grace Okafor

1. Result

What the change does to the authorization evidence of the earlier version.

1	18	0	176
Review required	Revalidate	Retired	Preserve

195 evidence requirements were examined. 176 (90.3%) carry forward unchanged. 19 are affected, across 11 requirements and 10 components. Reviewers have decided 194 of 195 dispositions; 1 is waiting.

2. What changed

6 differences between version 6 and version 7 of the system model.

Component	Attribute	From	To	Change class
Draft work orders AgentTool	`added`			`component.added`
FailurePredictor v3 Model	`version`	`3.3.0`	`3.4.1`	`model.version`
FailurePredictor v3 Model	`weightsHash`	`sha256:22c94e01b7aa`	`sha256:9f2c1e7a44d0`	`model.weights`
ManualAssistant pipeline PromptPipeline	`systemPromptHash`	`sha256:0a7e66d3b218`	`sha256:5b7e02d9c1aa`	`prompt.template`
ManualAssistant pipeline PromptPipeline	`templateVersion`	`13`	`14`	`prompt.template`
draft-to-workorders Data flow	`added`			`flow.added`

3. Components the change reaches

Direct: the component itself changed. Propagated: a component it depends on changed.

Component	Reach	How
Draft work orders AgentTool	Direct	component.added flow.added on flow draft-to-workorders upstream.modelBehavior via ManualAssistant pipeline > Draft work orders

Component	Reach	How
FailurePredictor v3 Model	Direct	model.version model.weights
ManualAssistant pipeline PromptPipeline	Direct	prompt.template
WorkOrderService Service	Direct	flow.added on flow draft-to-workorders neighbor.added via Draft work orders > WorkOrderService
AssistantAPI Service	Propagated	upstream.modelBehavior via ManualAssistant pipeline > AssistantAPI
Northwind AI government endpoint ExternalApi	Propagated	upstream.modelBehavior via ManualAssistant pipeline > Northwind AI government endpoint
Notification Service Service	Propagated	upstream.modelBehavior via FailurePredictor v3 > PredictionAPI > Notification Service
PredictionAPI Service	Propagated	upstream.modelBehavior via FailurePredictor v3 > PredictionAPI
Read technical manuals AgentTool	Propagated	upstream.modelBehavior via ManualAssistant pipeline > Read technical manuals
Web Portal Service	Propagated	upstream.modelBehavior via FailurePredictor v3 > PredictionAPI > Web Portal

4. Why: the rules that decided

Every recommendation names the rule that produced it. Rules are data in the signed rule pack named above.

Recommendation	Rule	Reason	Items
Review required	`PROMPT-TEMPLATE-BIAS`	Template changes can but do not always alter bias characteristics; an AI assurance lead decides whether the bias evaluation must be rerun.	1
Revalidate	`MODEL-BEHAVIOR-EVALS`	Evaluations, red-team results and the model card describe the prior model behavior and no longer reflect the changed model.	8
Revalidate	`PROMPT-TEMPLATE-EVALS`	Safety, injection resistance, task performance and robustness depend directly on the prompt.	4
Revalidate	`UPSTREAM-BEHAVIOR-EVALS`	This component's evaluated behavior depends on a model or pipeline that changed upstream.	3
Revalidate	`FLOW-ENDPOINTS`	The data flows of this component changed.	2
Revalidate	`PROMPT-TEMPLATE-REDTEAM`	Red-team results were obtained against the previous prompt and guardrails.	1
Preserve	`ENGINE-UNAFFECTED`	No change reached this component or the components this evidence depends on.	125
Preserve	`UPSTREAM-BEHAVIOR-DEFAULT`	Components downstream of a changed model keep their infrastructure and access evidence.	39
Preserve	`FLOW-DEFAULT`	Flow changes affect only connection, boundary and data protection evidence on the endpoints.	6
Preserve	`MODEL-BEHAVIOR-DEFAULT`	A change to model weights, version or training data does not affect infrastructure, access or configuration evidence for the model component.	3

Recommendation	Rule	Reason	Items
Preserve	PROMPT-TEMPLATE-DEFAULT	A prompt template change does not affect infrastructure, access or data evidence for the pipeline.	3

5. Requirements with affected evidence

Controls and AI requirements whose evidence must be redone or reviewed because of this change.

Requirement	Title	Revalidate	Review	Components
AC-4	Information Flow Enforcement	1		WorkOrderService
KAI-DOC-1	Model documentation	1		FailurePredictor v3
KAI-GEN-1	Prompt injection resistance	2		Read technical manuals, ManualAssistant pipeline
MANAGE-4.1	Post-deployment monitoring implemented	1		FailurePredictor v3
MEASURE-2.3	Performance measured for deployment conditions	2		FailurePredictor v3, ManualAssistant pipeline
MEASURE-2.5	Validity and reliability demonstrated	2		FailurePredictor v3, ManualAssistant pipeline
MEASURE-2.6	Safety risks evaluated	3		Read technical manuals, FailurePredictor v3, ManualAssistant pipeline
MEASURE-2.7	Security and resilience evaluated	3		Read technical manuals, FailurePredictor v3, ManualAssistant pipeline
MEASURE-2.10	Privacy risk examined	1		FailurePredictor v3
MEASURE-2.11	Fairness and bias evaluated	1	1	FailurePredictor v3, ManualAssistant pipeline
SC-8	Transmission Confidentiality and Integrity	1		WorkOrderService

6. Affected evidence and decisions

One row per piece of evidence that does not carry forward, with the reviewer's decision where one is recorded.

Evidence	Recommendation and rule	Owner	Decision
MEASURE-2.11 evaluation-run (bias) ManualAssistant pipeline	Review required PROMPT-TEMPLATE-BIAS	AI assurance lead	Waiting for a decision
KAI-DOC-1 model-card FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MANAGE-4.1 evaluation-run (drift) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.10 evaluation-run (privacy) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.11 evaluation-run (bias) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.3 evaluation-run (performance) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11

Evidence	Recommendation and rule	Owner	Decision
MEASURE-2.5 evaluation-run (robustness) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.6 evaluation-run (safety) FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.7 red-team-report FailurePredictor v3	Revalidate MODEL-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
KAI-GEN-1 evaluation-run (injection) ManualAssistant pipeline	Revalidate PROMPT-TEMPLATE-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.3 evaluation-run (performance) ManualAssistant pipeline	Revalidate PROMPT-TEMPLATE-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.5 evaluation-run (robustness) ManualAssistant pipeline	Revalidate PROMPT-TEMPLATE-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.6 evaluation-run (safety) ManualAssistant pipeline	Revalidate PROMPT-TEMPLATE-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.7 red-team-report ManualAssistant pipeline	Revalidate PROMPT-TEMPLATE-REDTEAM	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
KAI-GEN-1 evaluation-run (injection) Read technical manuals	Revalidate UPSTREAM-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.6 evaluation-run (safety) Read technical manuals	Revalidate UPSTREAM-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
MEASURE-2.7 red-team-report Read technical manuals	Revalidate UPSTREAM-BEHAVIOR-EVALS	AI assurance lead	Revalidate by Samuel Achebe, 2026-11-11
AC-4 data-classification WorkOrderService	Revalidate FLOW-ENDPOINTS	System owner	Revalidate by Grace Okafor, 2026-11-11
SC-8 transmission-encryption WorkOrderService	Revalidate FLOW-ENDPOINTS	Engineer	Revalidate by Grace Okafor, 2026-11-11

Evidence recommended to carry forward: 176. Confirmed by a reviewer: 176. Waiting for confirmation: 0. The full list is in the product and in the JSON form of this record.

7. Findings raised and reassessment work

The change raised no findings.

Reassessment task	Owner	Due	Status
Revalidate 1 data-classification item for CHG-0006	System owner	2026-11-25	Open
Revalidate 1 model-card item for CHG-0006	AI assurance lead	2026-11-25	Open
Revalidate 1 transmission-encryption item for CHG-0006	Engineer	2026-11-25	Open
Revalidate 12 evaluation-run items for CHG-0006	AI assurance lead	2026-11-25	Open
Revalidate 3 red-team-report items for CHG-0006	AI assurance lead	2026-11-25	Open

8. Determination

Completed by the responsible officials. Kendrake does not make this determination.

- ☐ No security impact. Authorization evidence carries forward as recorded above.
- ☐ Security-relevant change within the current authorization. Revalidate the evidence listed in section 6 and update the authorization package.
- ☐ Significant change. Refer to the authorizing official for a reauthorization decision.

Information System Security Officer: name, signature, date

Information System Security Manager: name, signature, date

System owner: name, signature, date

Authorizing official or designated representative: name, signature, date

Basis of this record

Kendrake Delta computed the recommendations in this record from the system model, the pinned rule pack and the evidence requirements of the earlier version. The same inputs always give the same result, identified by the analysis hash. Named reviewers made the decisions shown. The significance determination and any reauthorization decision belong to the responsible officials and are not made by this record.

Supports: NIST SP 800-53 Rev. 5, CM-4 Impact Analyses; NIST SP 800-53 Rev. 5, CM-3 Configuration Change Control; NIST SP 800-37 Rev. 2, Task M-1 System and Environment Changes; NIST SP 800-128, security impact analysis in configuration change control.

Appendix A. FedRAMP significant change notification worksheet

FedRAMP Consolidated Rules for 2026, Significant Change Notification, required information (SCN-CSO-INF)

Draft worksheet. The provider decides the change category, completes the remaining items and sends the notification. Check the current rule text before use.

No.	Required item	Entry
1	Service offering FedRAMP ID	Provider completes
2	Assessor name, if applicable	Provider completes
3	Related vulnerability, if applicable	Provider completes
4	Significant change type and explanation of categorization	Provider completes
5	Short description of the change	Assistant drafts work orders; FailurePredictor 3.4.1; prompt template 14 (CHG-0006: 6 differences between version 6 and version 7 of HARBORLIGHT Predictive Maintenance and Readiness Assistant).
6	Reason for the change	Provider completes
7	Summary of customer impact, including changes to services and customer configuration responsibilities	Provider completes
8	Plan and timeline, including verification, assessment or validation of affected controls	Revalidate or review 19 evidence items for AC-4, KAI-DOC-1, KAI-GEN-1, MANAGE-4.1, MEASURE-2.3, MEASURE-2.5, MEASURE-2.6, MEASURE-2.7, MEASURE-2.10, MEASURE-2.11, SC-8. 5 reassessment tasks opened, due by 2026-11-25. 1 reviewer decision still waiting.
9	Copy of the business or security impact analysis	This record, in PDF and JSON. Analysis hash b889a341cdf31410d6e7e92bbba8e284ed7a313b26a4d20b2bfb0d7c832fc0c1.
10	Name and title of the approver	Provider completes

Facts that bear on the change category

FedRAMP has the provider classify each significant change as routine recurring, adaptive or transformative. These facts come from the impact analysis. Kendrake does not choose the category.

- AI components added: Draft work orders (AgentTool).
- Existing AI components changed: FailurePredictor v3 (Model), ManualAssistant pipeline (PromptPipeline).
- Data flows: 1 added (draft-to-workorders), 0 removed.
- Reach: 10 components affected, 4 directly.
- Evidence: 176 of 195 items (90.3%) carry forward; 18 to revalidate, 1 for review, 0 retired, across 11 requirements.